



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2009-03

A burning need to know : the use of open source intelligence In the fire service

Robson, Thomas A.

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/4913>

Copyright is reserved by the copyright owner.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**A BURNING NEED TO KNOW: THE USE OF OPEN
SOURCE INTELLIGENCE IN THE FIRE SERVICE**

by

Thomas A. Robson

March 2009

Thesis Advisor:
Thesis Co-Advisor:

Richard Bergin
Robert Simeral

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE A Burning Need to Know: The Use of Open Source Intelligence in the Fire Service			5. FUNDING NUMBERS	
6. AUTHOR(S) Thomas A. Robson				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) <p>In the aftermath of September 11, 2001, the fire service found itself on the forefront of the war on terror. The people within the fire service began to realize they needed to share intelligence information with other government agencies in order to protect firefighters, and their community. At the federal level, the National Information Sharing Strategy recognized that first responders are critical to the prevention of terrorism and that an effective flow of intelligence information must be established between federal, state, local agencies.</p> <p>Yet, the fire service has little experience in the field of intelligence and much of the intelligence available may not be specific or useful to the fire service. The local fire department is faced with the task of analyzing what a particular piece of information means to that department. Only the local department knows its procedures and locale well enough to accomplish this critical task.</p> <p>This thesis seeks to assist local fire departments in building systems and training personnel to exploit open source intelligence for their unique needs. Using information gleaned from interviews with experienced intelligence people, the intelligence cycle is discussed including requirements, collection, analysis, and dissemination in light of the needs of the fire service.</p>				
14. SUBJECT TERMS Fire, Intelligence, Firefighter Training, First Responders, Fire Service Intelligence, Open Source Intelligence, Fire Service			15. NUMBER OF PAGES 97	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release distribution is unlimited

**A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE
IN THE FIRE SERVICE**

Thomas A. Robson
Battalion Chief, Fire Department, City of New York
B.S., Brooklyn College, 1980
D.D.S., New York University, 1984
M.A., University of Balamand, 2003

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2009**

Author: Thomas A. Robson

Approved by: Richard Bergin
Thesis Advisor

Robert Simeral
Thesis Co-Advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the aftermath of September 11, 2001, the fire service found itself on the forefront of the war on terror. The people within the fire service began to realize they needed to share intelligence information with other government agencies in order to protect firefighters, and their community. At the federal level, the National Information Sharing Strategy recognized that first responders are critical to the prevention of terrorism and that an effective flow of intelligence information must be established between federal, state, local agencies.

Yet, the fire service has little experience in the field of intelligence and much of the intelligence available may not be specific or useful to the fire service. The local fire department is faced with the task of analyzing what a particular piece of information means to that department. Only the local department knows its procedures and locale well enough to accomplish this critical task.

This thesis seeks to assist local fire departments in building systems and training personnel to exploit open source intelligence for their unique needs. Using information gleaned from interviews with experienced intelligence people, the intelligence cycle is discussed including requirements, collection, analysis, and dissemination in light of the needs of the fire service.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT.....	1
B.	RESEARCH QUESTION.....	3
C.	LITERATURE REVIEW.....	3
	1. History	3
	2. Open Source Intelligence.....	4
	3. Open Source Intelligence in Homeland Security	8
	4. The Intelligence Cycle	10
D.	ARGUMENT: MAIN CLAIMS, WARRANTS, EVIDENCE, AND CHALLENGES.....	13
E.	SIGNIFICANCE OF THE RESEARCH.....	15
II.	RESEARCH METHODOLOGY.....	17
A.	INTERVIEW PROTOCOL	17
B.	BIOGRAPHIES	19
	1. Fred Burton	19
	2. George Friedman	20
	3. Mark Johnson	20
	4. John McCreary.....	21
	5. Patrick Miller	22
C.	QUALITATIVE ANALYSIS	24
	1. Coding and Analysis	24
	2. Writing	28
III.	DATA ANALYSIS	31
A.	INTELLIGENCE	31
	1. Purpose	31
	2. Open Source Intelligence.....	33
	3. The Intelligence Cycle	34
B.	REQUIREMENTS.....	36
	1. Brainstorming	36
	2. Freedom	37
	3. Guidelines	38
C.	COLLECTION	42
	1. External Sources	42
	2. Internal Resources	47
D.	ANALYSIS	52
	1. Uncertainty	53
	2. Team Approach.....	53
	3. Operations.....	60
E.	DISSEMINATION.....	63
	1. Information Transfer.....	63
	2. Feedback	65

IV.	RECOMMENDATIONS.....	67
A.	TRAINING.....	67
1.	Formal Instruction	67
2.	Mentoring	69
B.	KEEPING IT REAL	70
V.	CONCLUSIONS.....	73
A.	PROPOSITIONAL MODEL.....	73
B.	INTELLIGENCE IN THE FIRE SERVICE.....	74
	LIST OF REFERENCES.....	77
	INITIAL DISTRIBUTION LIST	81

LIST OF FIGURES

Figure 1.	Emergent Analytical Codes and Categories	28
Figure 2.	Stages of the Intelligence Cycle: Description and Representative Quotes.....	35
Figure 3.	Propositional Model	74

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS

ACLU		American Civil Liberties Union
CIA	Central	Intelligence Agency
DIA	Defense	Intelligence Agency
DHS		U.S. Department of Homeland Security
DNI	Director	of National Intelligence
EMT	Emergence	Medical Technician
FBI		Federal Bureau of Investigation
FDNY		Fire Department, City of New York
FDSOA		Fire Department Safety Officers Association
FOUO		For Official Use Only
FSIE		Fire Service Intelligence Enterprise
IED	Improvised	explosive device
NYPD		New York City Police Department
OI&A		DHS Office of Intelligence and Analysis
OSAC	Overseas	Advisory Council
OSC	U.S.	Open Source Center
OSINT		Open source intelligence
PSA	Protective	Security Advisor
SME	Subject	matter expert
Stratfor		Strategic Forecasting, Inc.
SWAT	Special	Weapons and Tactics
TLO	Terrorist	Liaison Officer
USCG	U.S.	Coast Guard

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Before all I acknowledge Him who strengthens me.

I want to thank Joan for putting up with all of this. Thank you for all the love and support.

I would like to express my sincerest gratitude to Richard Bergin and Robert Simera for their invaluable advice on this thesis.

I am also extremely grateful to Fred Burton, George Friedman, Mark Johnson, John McCreary, and Patrick Miller for taking time out of their busy lives to be interviewed by me.

In addition, I want to express my heartfelt thanks to Battalion Chief Frank Montagna for all of his assistance on this project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Traditionally, the fire service was not a consumer of open source intelligence, nor was the processing of counterterrorism intelligence considered a normal function of local fire departments. However, in the aftermath of the September 11, 2001 attacks, the fire service suddenly found itself on the front row of the war on terror with a need to receive vital intelligence. This need for supplying information to local governments, including local fire departments, was also recognized on the national level. Many federal documents, especially Executive Order 13356, seek to strengthen the sharing of counterterrorism intelligence between federal entities and local governments. Further, the National Information Sharing Strategy recognizes that first responders are critical to the prevention of terrorism and that an effective and efficient flow of intelligence information must be established between federal, state, local, and tribal authorities.¹ Additionally, some fire departments such as the Fire Department of the City of New York (FDNY) seek to establish efficient information transfer arrangements between it and other governmental entities.² The ultimate goal of this intelligence sharing effort is the prevention or mitigation of terrorist attacks on the United States and the local community.

“Open Source Intelligence or OSINT is unclassified information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question.”³ For the fire service, the specific question to be answered is how is what is happening in the field of terrorism going to affect its operations, the safety of its personnel, and the safety

¹ *National Strategy for Information Sharing* (Washington, D.C.: The White House, October 2007), 3.

² *Terrorism and Disaster Preparedness Strategy* (New York: Fire Department of the City of New York 2007), 20.

³ *NATO Open Source Intelligence Handbook* (North Atlantic Treaty Organization, November 2001), v.

of the people they serve. For instance, information available on a jihadi website might show an increase in the use of secondary devices during jihadi attacks. When discovered and disseminated to fire department units this intelligence may save the lives of firefighters and the citizens they are sworn to protect. Currently, the fire service is not guaranteed access to this information or it is subject to such a large flow of information that this critical nugget of intelligence may be overlooked.

Additionally, since most fire department personnel do not have security clearances, the most useful type of intelligence information is open source intelligence (OSINT), especially since most fire departments will want to disseminate intelligence information to all of its members. "Due to its unclassified nature, OSINT can be shared extensively without compromising national security."⁴ The difficulty encountered with the reception of open source intelligence is that the fire service is generally not currently equipped to handle it. Assuming the local fire department is receiving intelligence, the flow of information coming out of the Federal government and local fusion centers is massive and requires additional processing by fire departments to exploit this intelligence properly. Additionally, much of the information flow may not be specific or useful to the fire service. Much of it tends to be for use by the law enforcement community. Therefore, though the fire service may receive large amounts of open source information, it will not necessarily obtain a large amount of OSINT for most of the information received will be valueless. Hence, the local fire department needs to separate out what it finds useful from this information flow. This is called the signal-to-noise problem. Therefore, local fire departments need specifically trained personnel and systems to accomplish this processing and analysis. Most fire departments do not have the systems or the personnel in place to exploit this information flow, nor do they have the

⁴ Eliot Jardines, *Using Open Source Information Effectively: Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security of the House of Representatives June 21, 2005* (Washington, D.C.: U.S. Government Printing Office, 2007), 13.

experience to build such systems. The proposed thesis will research the building of processes, and systems to obtain, process, and evaluate open source intelligence efficiently for use by the fire service.

B. RESEARCH QUESTION

How could local fire departments build systems and train personnel to exploit open source intelligence for their unique needs?

C. LITERATURE REVIEW

1. History

Since the fire service is a new player in the intelligence field, there is little written about its role or its usage of intelligence. However, the first fire department formally to look at the use of intelligence to support its operations was the Fire Department of the City of New York (FDNY). After the September 11, 2001 attacks, the FDNY realized it needed situational awareness and intelligence on terrorism to prepare, respond, and recover better from a possible attack. The FDNY formalized its vision in its 2007 document *Terrorism and Disaster Preparedness Strategy*. The strategy states, "Terrorists have proved they are extremely adaptive and reactive to changes in the security environment. Therefore, to be truly prepared for terrorist incidents the Department must be adaptive to new threats . . ." ⁵ To this end, the FDNY began to meet with the Department of Homeland Security in order to discuss information and intelligence sharing. "The Department of Homeland Security's Office of Intelligence and Analysis (OI&A) and the Fire Department of the City of New York (FDNY) met in New York in fall of 2006 to discuss fire service writ large as partners in sharing homeland security information. Both agencies agreed about the vital need to share information for the security of the Nation against enemies' hostile

⁵ *Terrorism and Disaster Preparedness Strategy* (New York: Fire Department, City of New York, 2007), 10.

intentions (counterterrorism information).”⁶ Additionally, both agencies agreed that other fire departments should be brought into the Fire Service Intelligence Enterprise in order to share information horizontally as well as vertically. In addition, if fire departments kept each other informed of what is occurring in their locality, seemingly isolated incidents may show a pattern that indicates terrorist activity. To that end, fifteen major city fire departments have agreed to form a trusted network, a “community of interest” to share intelligence and lessons learned.⁷

Several theses have recently come out of the Naval Postgraduate School discussing various aspects of intelligence in the fire service. Much of the emphasis has been on the role of the firefighter as an intelligence collector. Additionally, the Center for Policing Terrorism released a report recommending the fire service “serve a preventive intelligence role.”⁸ Other theses have recognized the need for the fire service to move from a reactive to a proactive posture by the use of intelligence in planning and training.

2. Open Source Intelligence

Open source intelligence or OSINT seeks to analyze information found in television broadcasts, radio broadcasts, newspapers, the internet, academic and scientific journal articles, commercial data, non-secret foreign governmental reports, and speeches by foreign politicians. OSINT, by definition, is not collected by illicit means. The advantage to using open source intelligence to the American fire service is that most of its members do not have security clearances. OSINT may be widely distributed within a department with only an “sensitive but unclassified” or a “for official use only” caveat. Some agencies use an additional caveat “law enforcement sensitive” for certain specialized materials

⁶ Fire Service Intelligence Enterprise (FSIE): *Progress Report 1*, (U//FOUO) (December 28, 2007), 2.

⁷ Ibid., 4.

⁸ Kyle Dabruzzi and Daveed Gartenstein-Ross, “Firefighters’ Developing Role in Counter Terrorism,” *Policing Terrorism Report 3* (July 2008), 5.

that demand additional dissemination restrictions; however, the distinctions within the field of “sensitive but unclassified” materials are somewhat artificial. Intelligence marked “secret” and “top secret” may be advantageous to the highest levels of a department; however, it will never allow situational awareness for the rest of a department unless it can be “sanitized” to unclassified. OSINT may also inform higher echelons of a fire department about what information they are lacking, allowing them to go to the federal government for additional information or clarification.

What is the value of OSINT? The literature shows that for many traditional analysts, open source information was a starting point in the collection or analysis of other forms of intelligence. OSINT is thought to create a background for the analyst to help him or her understand the issues and people involved in a particular matter. However, OSINT can also be used to verify or supplement other intelligence sources.⁹ Additionally, foreign newspapers and speeches made by a terrorist organization’s higher-level leadership may give a window into the collective mind of these groups. Speeches and articles written by foreign policy makers may also provide insight into their hopes and concerns as well. It may be useful in the evaluation of societal and economic trends. It may be used to track dual-source technology that could be used in the production of WMDs and its supply network. Yet another benefit to OSINT is that since it is derived from open sources, it may be possible to release the intelligence to foreign leaders or the press if beneficial to the United States without revealing its classified sources and methods.

There is another area of OSINT sources called “gray literature.” Gray literature consists of limited availability materials where there are few copies produced. Alternatively, the existence of this type of literature may be for the most part unknown or has a restricted distribution through specific channels. These materials may consist of “working papers, pre-prints, technical reports and

⁹ *Open Source Intelligence*, (U//FOUO) (Washington, D.C., Department of the Army, December 5, 2006), 2-2.

technical standards documents, dissertations, data sets, and commercial imagery,” internal use only documents and articles, journals, and reports prepared for specific organizations or associations.¹⁰ This literature is, by its very nature, difficult to search for and acquire; for instance, some trade literature available at a show and papers delivered at a conference may only be distributed to those at the trade show or conference.¹¹

OSINT has several limitations. One is that an analyst will rarely find information that foreign governments are trying to hide in open sources. In other words, you will not generally find secrets there. OSINT will, therefore, rarely supply the “smoking gun” about some issue or threat.¹² Consequently, OSINT may not be a replacement for other forms of intelligence. It relies on information that is fragmentary and open to various interpretations. This means OSINT must be fit into the larger picture. Due to the volume of the data flow, policy makers must understand that the OSINT analyst may completely miss important information.

As was mentioned previously, one of the problems with creating OSINT is that the amount of raw information available is voluminous and even with sophisticated software, it still requires many resources to translate, cull, and convert it into a form that can be useful in generating intelligence. OSINT analysts will look for a wide range of information, ideally, from many different types of open sources in an effort to confirm a possible piece of intelligence. However, having a large amount of open source information will not necessarily give you a large amount of OSINT for most of the information received will be

¹⁰ *NATO Open Source Intelligence Handbook* (North Atlantic Treaty Organization, November 2001), 8.

¹¹ *NATO Open Source Intelligence Reader* (North Atlantic Treaty Organization, February 2002), 25.

¹² Jennifer Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, D.C.: Georgetown University Press, 2005), 67.

valueless (the signal-to-noise problem or “wheat and chaff problem”).¹³ The rest must be “filtered” and, ideally, verified before it can be passed on to other analysts, department policy makers, or personnel.

An additional problem with OSINT is that, though there can be a collection strategy, the analyst has no ability to task its collection as can be done with the other “INTs.” For example, the analyst cannot control what foreign newspapers will print, or what speeches terrorist groups will make, which means the information the OSINT analyst needs may or may not be available when he or she needs it. The analyst must, instead, sit by their stream of information and see what type of fish they hook. This leads to a further complication, since the analyst has no control over its production, they must be careful in the intelligence vetting process because the open source information received may be disinformation or propaganda placed there by foreign governments. However, for every major or minor event in the world, at least 20 independent sources report on the very same event.

The risk and possibility of misinformation or deception have grown, but the risk also has been reduced. It has become harder for remote and closed areas of the world to keep things secret and to fool its own citizens with propaganda.¹⁴ Additionally, since open source information is available to everybody, there will be pressure to release some analysis before, for instance, the *New York Times* does. However, the OSINT analyst must not rush this vetting process, or the risk of creating incorrect intelligence increases.

¹³ Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006), 102.

¹⁴ *NATO Open Source Intelligence Reader* (North Atlantic Treaty Organization, February 2002), 80.

3. Open Source Intelligence in Homeland Security

“In today’s complex and dangerous world, US policy makers need contextual, contemporary, and relevant knowledge to make decisions.”¹⁵ This is most certainly true of the leadership of the fire service in the United States. In the effort to protect the homeland, whether from natural disasters or from terrorist attack, firefighters will be sent into harm’s way. Their departments and the national government owe them the best training, information, and equipment available. Training firefighters to respond to terrorist incidents can only be done if the leadership of a department has information at hand to plan and execute training properly. The same is true for the types of equipment a department might purchase. Similarly, current situational awareness is critical to the safety of firefighters. Awareness of an impending attack could lead to an increase of staffing or changes in firefighting procedures and response patterns. Firefighting is an inherently dangerous occupation; no amount of information can eliminate those risks. However, intelligence about the current terrorism landscape and its future possibilities can reduce those risks to the extent possible.

In his testimony before the U.S. Congress on the value of OSINT in the realm of homeland security, Eliot A. Jardines stated, “From Pearl Harbor to the September 11th terrorist attacks, intelligence failures have largely resulted not from a lack of information, but rather the inability to effectively disseminate that information or intelligence.”¹⁶ Others posit, “major intelligence failures are usually caused by failures of analysis.”¹⁷ He also points out that the use of OSINT effectively bypasses the problem of obtaining security clearances for each first responder. “In fact, OSINT products could be disseminated to the full complement of first responders such as firefighters, EMTs, university police

¹⁵ Eliot A. Jardines, *National Open Source Enterprise* (Washington, D.C.: Office of the Director of National Intelligence, April 2006), 6.

¹⁶ House Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, *Using Open Source Intelligence Effectively*, 109th Cong., 1st sess., 2005, 13.

¹⁷ Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, D.C.: Center for the Study of Intelligence, 1999), 65.

departments, hospitals, and private security firms. Consider for a moment what a paradigm shift that would represent.”¹⁸ It is important to note here that a fire department analyzing its own needs and requirements and attempting to fulfill those requirements does not mean cutting itself off from other sources of information such as federal and state governments. For instance, Charles Allen reported, “DHS Intelligence is developing a strong Open Source Intelligence (OSINT) capability focused on our areas of expertise and responsibility to complement the broader Intelligence Community’s open source investments.”¹⁹ Fire departments will continue to be dependent on these sources as well. Indeed, fire departments developing products for their internal use may want to release them through DHS because they may be of real interest to other members of the fire service.

The testimony before the committee also made it clear that open source intelligence is not a panacea nor can it be separated from other sources of intelligence.²⁰ However, it is the best way to ensure homeland security intelligence is as widely distributed as possible. Wide distribution ensures that homeland security intelligence is in the hands of the people who can tactically use it. A United States Navy Air Wing Commander leading the first flights over Baghdad said, “If it is 85% accurate, on time, and I can share it, this is a lot more useful to me than a compendium of Top Secret Codeword material that is too much, too late and needs a safe and three security officers to move it around.”²¹ This is true for homeland security intelligence as well. Produced materials should be kept at a “For Official Use Only” level to ensure some level of security. In addition, individual fire departments need to be able to use open source materials without violating an individual’s Constitutional rights.

¹⁸ House, Committee, *Using Open Source Intelligence Effectively*, 14.

¹⁹ Senate Select Committee on Intelligence, *Intelligence Reform, and Homeland Security Intelligence*, 110th Cong. 1st sess., 2007, 4.

²⁰ House Committee, *Using Open Source Intelligence Effectively*, 4.

²¹ Robert David Steele, *Open Source Intelligence: Executive Overview* (Global Intelligence Partnership Network, January 1, 2004), 21, <http://www.oss.net/> (accessed April 18, 2008).

4. The Intelligence Cycle

The literature shows that proper intelligence, including open source intelligence, is an iterative process. The various steps in the intelligence process are distinct, but inseparable, if good intelligence products are to be delivered. This progression is called the intelligence cycle. There are several models of the intelligence cycle, however, all the models really involve the same concepts. For instance, even within the U.S. Army, there are different models in the literature. The model that appears in the U.S. Army's *Open Source Intelligence* manual describes a five-step model for the exploitation of open source intelligence. The five steps in this model are planning, preparing, collecting, processing, and production.²² The U.S. Army Intelligence Center's guide, *Targeting Tomorrow's Terrorist Today*, describes five steps beginning with Planning and Direction. At this step, the possible sources of OSINT information is identified. Then comes the Collection phase in which the actual data is captured. The data is then run through the Processing, Integration, and Guidance phase. Then, hopefully, validated intelligence is analyzed and intelligence products produced in the Analysis and Production phase. Finally, the product reaches the Dissemination phase. At this phase, the level of restriction is decided since finished products may divulge OSINT collection capabilities.²³

The United States Department of Justice's Bureau of Justice Assistance describes a six step cyclical process.²⁴ These steps consist of "Planning and Direction," in which this step leads to the actual Collection phase; for law enforcement, this is the most labor-intensive aspect of the intelligence

²² *Open Source Intelligence, FMI 2-22.9 (U//FOUO)* (Washington, D.C., Department of the Army, December 5, 2006), 3-1.

²³ Ben Benavides, *Targeting Tomorrow's Terrorist Today (T⁴) through Open Source Intelligence (OSINT): Quick-Links Started Handbook for the Open Source Analyst*, (U//FOUO) (Fort Huachuca: U.S. Army Intelligence Center, January 2007), 48.

²⁴ *The National Criminal Intelligence Plan* (Washington, D.C.: US Department of Justice, June 2005), 3, http://www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf (accessed July 10, 2008).

process.”²⁵ The information goes through a Processing/Collation phase. The results of that phase are put through an Analysis phase. Of course, analysis for law enforcement may be very different from either a national intelligence organization or a fire department. Police analysis should produce intelligence that gives leads in an investigation or results in prosecution, in addition to preparation for and prevention of terrorist attacks.²⁶ The product is then disseminated to those within the organization who need to know it. Reevaluation of the intelligence is then carried out resulting in a new period of planning and direction.

Other authors such as Lowenthal propose a seven-step intelligence process.²⁷ The first step in the seven-step process is identifying requirements. Requirements are the items that the open source process is supposed to clarify or on which to capture information. Within the Fire Service Intelligence Enterprise (FSIE), there is a Requirements Working Group, which is beginning to identify the requirements of the fire service. These fall into five broad categories. The first category of requirements is potential incidents and threats. The second requirement was time estimates as these can directly impact situational awareness and operational readiness.²⁸ Third, what are the general protective measures being taken by other agencies and levels of government.²⁹ The fourth requirement is such information that “informs fire service actions” such as protecting firefighters, their families, operations, and mission.³⁰ The last

²⁵ *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, D.C.: US Department of Justice, September 2005), 6, <http://www.ncjrs.gov/pdffiles/lesl/bja/210681.pdf> (accessed July 7, 2008).

²⁶ Ibid.

²⁷ Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006), 102.

²⁸ Fire Service Intelligence Enterprise (FSIE): *Progress Report 1*, (U//FOUO) (December 28, 2007), I-2.

²⁹ Ibid., I-3.

³⁰ Ibid.

requirements set identified was information on special events, target hazard analysis, natural disaster vulnerability and prediction, and cyber threats.³¹

This effort by the Fire Service Intelligence Enterprise to identify the common requirements of the fire service was necessary because homeland security intelligence is dominated by law enforcement, while the needs of the fire service may be quite different. "Several SMEs (subject matter experts) cited the overall lack of inclusion of these other disciplines (public health, fire, emergency medical services, and private sector security) at all levels as a critical shortcoming in the development of comprehensive, effective information and intelligence sharing processes."³²

The next identified step in the intelligence cycle is collection. Collection is how the necessary information to fulfill the identified intelligence requirement is obtained. It is important to note that all that is being collected here is information, raw data if you will; this information is of little value until it is processed and analyzed. Requirements should give those tasked with producing the necessary intelligence a sense of how critical that particular requirement is. This allows the organization and the individual analyst to assign a priority to its collection. Without such information, critical requests may be delayed because the analyst is attempting to fulfill a request for intelligence that has little or lesser criticality.

The following step, Processing, seeks to eliminate superfluous and incorrect material and to arrange the data in a logical format.³³ In other words, the information is vetted and organized. Only then can an analyst begin to attempt to create a coherent picture out of the available information. This is where information and data become intelligence. Intelligence can be considered

³¹ Fire Service Intelligence Enterprise (FSIE): *Progress Report 1*, (U//FOUO) (December 28, 2007), I-3-4.

³² U.S. Department of Homeland Security Lessons Learned Information Sharing, *LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process* (December 2005), 4.

³³ *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, D.C.: US Department of Justice, September 2005), 7, <http://www.ncjrs.gov/pdffiles/lesl/bja/210681.pdf> (accessed July 7, 2008).

a “concisely tailored answer reflecting a deliberate process of discovery, discrimination, distillation, and delivery of data precisely suited to need.”³⁴ In other words, intelligence is an answer to a question asked by a policy maker, which draws upon known data and information, but put through a refinement process that adds value to existing information by the input of the analyst. The next part of the intelligence cycle is Dissemination; here, the finished product is moved to the people who requested it or can use the material. For instance, some product may be produced for the higher echelons of an organization for long-term planning and materials acquisition. This would be strategic intelligence. Other intelligence may be for day-to-day situational awareness. This is an example of tactical intelligence.

The sixth step, Consumption is important as well. Consumption means that the people who were supposed to read the prepared and disseminated intelligence actually read it. Finally, the people who read the intelligence respond to it. In an ideal world, they let the people who prepared the intelligence know, “what has been useful, what has not, which areas need continuing or increased emphasis, which can be reduced and so on.”³⁵ Additionally, the intelligence product may raise additional questions in the consumer’s mind, which, in turn, may lead to further requests for intelligence. These new requirements start the intelligence cycle again.

D. ARGUMENT: MAIN CLAIMS, WARRANTS, EVIDENCE, AND CHALLENGES

September 11, 2001 changed the world in many ways. Agencies, such as the local fire department, that had never considered themselves targets of terrorist attacks, now found themselves on the front line of defending their country and their community against terrorist attacks. This was new and

³⁴ Robert David Steele, *Open Source Intelligence: Executive Overview* (Global Intelligence Partnership Network, January 1, 2004), 3, <http://www.oss.net/> (accessed April 18, 2008).

³⁵ Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006), 64.

uncharted territory to the fire service. The ability of the fire service to execute its sworn duty to protect life and property in the local community, as well as, to the extent possible, protect the firefighters who serve there from the consequences of terrorism, is dependent on the efficient usage of intelligence. The fire service requires homeland security intelligence for everything from planning to response and mitigation. Fire departments, out in the community on building inspections or responding to routine emergencies, may be able to prevent terrorism with good intelligence that leads to situational awareness. Currently, most fire departments have no systems in place for effectively collecting, analyzing, and dissemination open source intelligence for their own use. Developing a system wherein fire departments can properly exploit useful open source intelligence would enhance firefighter safety and add to their ability to prevent terrorism in their community and more efficiently respond to and mitigate such an attack if it occurred.

Some might argue that having an in-house system in the local fire department to exploit open source intelligence is wasteful or unnecessary or both as counter-terrorism intelligence may be supplied by the Department of Homeland Security's Office of Intelligence and Analysis or by their local police department or by their regional fusion center. Evidence will show that while these flows of information are not to be ignored, they are primarily law enforcement oriented and not necessarily useful to a local fire department. In addition, the flow of intelligence from the above-mentioned agencies must still be further analyzed to discover what is most applicable to the local fire department. The needs of the fire service are different from other agencies. Others might posit that the Fire Service Intelligence Enterprise (FSIE) will solve a local departments intelligence needs. The FSIE is certainly a step in the right direction; however, this system still does not address the needs of the fire department in its local community. An additional alternative might be to place fire service personnel in the local fusion center. However, in some areas where a local fusion center per se does not exist and given the uneven quality and intent of local fusion centers, this may not be a viable alternative.

E. SIGNIFICANCE OF THE RESEARCH

The immediate consumers of this research will be fire departments and other government agencies that are non-traditional consumers of open source intelligence such as public health entities. The research will lay out a “game plan” by which fire departments can effectively develop, disseminate, and employ open source intelligence to support prevention, planning, and operations in the post 9-11 environment. The research will also be useful to government agencies that might be tasked with supporting the fire service with homeland security orientated intelligence. Homeland security practitioners will gain insight into setting up an effective system for the collection and use of OSINT in agencies outside the intelligence and law enforcement communities. Finally, private entities, such as hospitals, and utilities, may find this research valuable in creating intelligence systems useful with a view to protecting their facilities from a terrorist attack or dealing with the after effects of such an attack.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RESEARCH METHODOLOGY

This thesis will study the use of intelligence in the fire service from a qualitative research approach. The study will use qualitative interviews focused on understanding processes and building the frameworks required for a fire department to use intelligence in order to protect life and property in the community they serve. This is what is referred to in the literature as “topical interviews.”³⁶ What is most important here is for the researcher to find subject matter experts of sufficient experience as to be able to shed light on a particular problem or issue. In this particular case, little research has been done on the problem of intelligence use by the fire service, so the researcher must interview experts in other fields of intelligence and apply the knowledge gained to a fire department intelligence unit.

A. INTERVIEW PROTOCOL

The problem of intelligence use by the fire service was studied by qualitative analysis because the field is not well researched, which means it is difficult to “generate hypotheses and develop quantitative measures.”³⁷ To this end, five interviews of approximately one hour each were conducted with subject matter experts (SMEs) in the field of intelligence. Each SME had a minimum of fifteen years of experience in the intelligence field. Indeed, the average length of experience with intelligence is over 20 years. Interviewees were intentionally drawn from a wide range of intelligence backgrounds so that the problem of intelligence use in the fire service could be viewed from a variety of perspectives. Two interviewees serve with the federal government. One has a background in open source intelligence; the other has a forty-year background in military

³⁶ Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data 2nd ed.* (Sage Publications, Thousand Oaks, CA, 2005), 11.

³⁷ Gail Fann Thomas, “Research Methods: Qualitative Data Analysis,” 2, https://www.chds.us/courses/file.php/279/lecture_transcript/6-res_methods_qual_data_analysis_transcript.doc?forcedownload=1 (accessed January 22, 2009).

intelligence. The third interviewee is a senior level chief in local law enforcement and has a thirty-three year background in police intelligence. Two have a background in private sector intelligence. The researcher conducted initial interviews between November 4, 2008 and November 25, 2008. The researcher personally performed all depth qualitative interviews. They were all conducted by telephone and recorded for accuracy. The interviews were later professionally transcribed into a Word document format.

The interviews were started by using what Rubin and Rubin referred to as a “hypothetical example.”³⁸ The question was, “If you suddenly found yourself tasked with the mission of starting a fire department intelligence unit from scratch, how would you go about it?” This question was designed to allow the interviewee to talk freely about their take on the issue of the research question. Additionally, broadly worded main questions were prepared as a framework to insure all concepts gleaned from the literature were covered and that each part of the topic was thoroughly explored.³⁹ These follow-up questions were allowed to evolve as each prior interview was analyzed. This process of theoretical sampling was continued until all five interviews were completed. Theoretical sampling kept the interviewing process open to changes in direction as indicated by the data itself.⁴⁰ In addition to the main and follow-up questions, continuation probes were used to expand the depth of detail and elaboration probes were used to connect and further explore the themes and concepts covered by the main question. From the existing data, gaps were noted and follow-ups to the interviews were carried out via e-mail. Answers to follow-up interviews were received between November 26, 2008 and January 19, 2009.

³⁸ Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data 2nd ed.*, (Sage Publications, Thousand Oaks, CA, 2005), 161.

³⁹ Ibid., 135.

⁴⁰ Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research*, 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 144.

B. BIOGRAPHIES

1. Fred Burton

Mr. Burton is one of the world's foremost authorities on security, terrorists, and terrorist organizations. In his capacity as Vice President for Counterterrorism and Corporate Security at Stratfor, Mr. Burton oversees the firm's terrorism intelligence service and consults with clients on security-related issues affecting their organizations or personal safety. He leads a team of terrorism experts and a global network of human intelligence sources to analyze and forecast the most significant events and trends related to terrorism and counterterrorism.

Mr. Burton is the author of *Ghost: Confessions of a Counterterrorism Agent*, a story of his role in the burgeoning terrorist threat in the 1980s and beyond.

Before joining Stratfor, Mr. Burton served as a special agent in counterterrorism for the U.S. Department of State, where he was involved with many high-profile operations. He orchestrated the arrest of Ramzi Yousef, mastermind of the first World Trade Center bombing, and investigated cases such as the assassination of Israeli Prime Minister Yitzhak Rabin, the killing of Rabbi Meir Kahane, the al Qaeda New York City bombing plots before 9/11, and the Libyan-backed terrorist attacks against diplomats in Sudan and Khartoum. He has also served as the U.S. liaison officer to several international security, intelligence, and law enforcement agencies, providing consulting on global intelligence and threat identification.

In addition, Mr. Burton has revolutionized the field of security by designing a unique and specialized protective program to safeguard CEOs, their families, employees, and physical facilities. His strategy is highly valued and has been implemented by governments and a number of the world's leading corporations.

2. George Friedman

Dr. Friedman is the founder and Chief Executive Officer of Stratfor (www.stratfor.com), a company he began in 1996 that is now a leader in private intelligence. Dr. Friedman guides Stratfor's strategic vision, helping shape the firm's long-range geopolitical forecasts as well as overseeing and tasking tactical intelligence operations.

Dr. Friedman is also the author of numerous articles and books on national security, warfare, and intelligence. His most recent book, *America's Secret War*, a *Barron's* Best Book of 2004, describes America's covert and overt efforts in the global war on terror. Dr. Friedman's next book, *The Next Hundred Years: a Forecast for the 21st Century*, is set for a January 2009 release.

Major television shows and radio programs such as CNN's *Lou Dobbs*, Fox News' *The O'Reilly Factor*, and NPR frequently invite Dr. Friedman to appear as a national security and international affairs intelligence expert. *Barron's* has cited Stratfor's analysis on numerous occasions and *Barron's* cover article featured an interview in October 2001. He has also been featured in *Time* magazine, *The New York Times* and the *Wall Street Journal* and quoted in reference to global issues in the *New York Times*, *USA Today*, *Fortune*, *International Herald Tribune* and many other domestic and international publications. Dr. Friedman has been the keynote speaker at numerous conferences and industry specific events for private organizations and government agencies.

Dr. Friedman received his bachelor's degree from the City College of the City University of New York and holds a Ph.D. in government from Cornell University.

3. Mark Johnson

Mr. Johnson is the Enterprise Partnership Manager for Homeland Security in the Open Source Center. In this role, Mr. Johnson interacts with homeland security related components of the federal, state, and local governments for the

U.S. Director of National Intelligence (DNI) Open Source Center (OSC). In this recently created position, Mr. Johnson seeks to facilitate relationships that will leverage all forms of openly available information to result in homeland security insights, actions, and impact. Open source intelligence includes: text, broadcast, video, data, geographic, and internet derived information. Open Source intelligence is a valuable source for analytical understanding, early warning, tip-offs, and event detection and tracking—especially topics with a foreign aspect impacting homeland security, such as terrorism, biological hazards, cyber threats, weapons of mass destruction, and narcotics trafficking.

Mr. Johnson is a professional geographer, intelligence officer, former U.S. Army officer, and senior manager whose 28-year federal career has centered on the use, collection, exploitation, and creation of open source information. Prior to his current assignment, Mr. Johnson directed the only center in the U.S. intelligence community focused solely on open source geospatial materials—the OSC Map Services Center. His assignments over the years have taken him from Bangor to Baghdad, Tucson to Tokyo and points in between. Mr. Johnson holds a Master of Information Systems from Virginia Tech and has frequently written, taught, and spoken on intelligence topics.

4. John McCreary

John F. McCreary is a distinguished 38-year veteran of defense intelligence. He is the author of the internationally acclaimed, nightly news commentary, NightWatch™. He has taught strategic analysis and warning to the intelligence staffs of 32 countries. He created and taught the U.S. National Warning Course from 1983 to 1992. Since October 1, 2008, he has served as the Highly Qualified Subject Matter Expert for Analysis Transformation for the United States Air Force Intelligence Analysis Agency.

Mr. McCreary has worked intelligence for both the U. S. Government and in private industry. From June 2006 to May 2008, Mr. McCreary was employed by dNovus RDI as Director of National Intelligence and Analysis and was

appointed Vice President for Intelligence Analysis in May 2007. He served the United States government from 1968 to May 2006 as an intelligence analyst with the Defense Intelligence Agency. From 1998 to May 2006, he served as Senior Level Expert for current intelligence and strategic warning, with the rank of SES/SL-4; senior intelligence advisor in the Joint Staff; senior intelligence analyst in the Defense Intelligence Agency. From 1993 to 1998, Mr. McCreary served as Senior Intelligence Officer for Asia, Directorate of Intelligence, J2, Joint Staff.

From 1998 to date, Mr. McCreary publishes *NightWatch*, an executive style, nightly analysis of significant international events with impact on U.S. national security. He has also written "The Latest Intelligence Crisis," with Richard A. Posner in *Intelligence and National Security*, Volume 23, in 2008, *Intelligence as Evidence*, a J2 monograph published in 1996, *Analysis of Political Instability*, a J2 monograph published in 1995 and "Warning Cycles" in *Studies in Intelligence* in 1983.

Mr. McCreary has received multiple commendations, citations, medals, and awards from the Intelligence Community, the CIA, and the DIA. In 2004, he received a Presidential Rank Award for Meritorious Service, the only DIA analyst to ever have received this award. He graduated magna cum laude from the University of Illinois in 1968, majoring in Chinese and European history and graduated from Georgetown University Law Center, with the degree of Juris Doctor (JD) in 1975. He is also a member of the Georgetown University Law Journal.

5. Patrick Miller

Chief Miller has served thirty-three years with the Ventura California Police Department and currently serves as its chief. Chief Miller developed the Ventura Police Department's Intelligence-Led Policing Program and a County Terrorism Working Group. Over the years, Chief Miller has served the Ventura Police Department in a variety of ranks and roles, including Intelligence, SWAT,

Narcotics, and Field Task Forces. Additionally, Chief Miller has taught for over 25 years in the law enforcement field including Homeland Security, Leadership, Terrorism, Narcotics, Intelligence, and Criminal Law.

In addition, from 1986 to the present, Chief Miller has worked on special assignments for the Central Intelligence Agency. Chief Miller worked as a full-time case officer and on a contract basis on a variety of classified intelligence operations in Central and South America, including training, handling assets, preparing intelligence reports and briefs, and performing classified operational duties. He wrote or led policy development and implementation of U.S. Government counter-narcotics programs in Columbia and El Salvador in 1986 – 1988. Since 2001, Chief Miller has served on numerous panels and committees

Regarding terrorism, asymmetrical warfare, low-intensity conflict, insurgency, and threat assessment. Since 1993, he has been a guest lecturer at the CIA training facility at Camp Perry Virginia.

Chief Miller is on the editorial board of an internal CIA publication. He has been involved with authoring *Using Tactical Intelligence, Internal CIA Publication* in 1995, and *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement* in 2005. He was also involved with authoring *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*, and *Developing and Sharing Information and Intelligence in a New World: Fusion Center Guidelines*, also in 2005, and *A Law Enforcement Assistance and Partnership Strategy: Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement* in 2006.

Chief Miller received a Master's of Public Administration from Pepperdine University in 1980, completed the California Command College at the California Polytechnic University in 1996, and received a Master of Arts from the Naval Postgraduate School in Security Studies (Homeland Defense and Security) in 2005.

C. QUALITATIVE ANALYSIS

Qualitative analysis of these interviews used open coding hand-in-hand with axial coding.⁴¹ Theoretical memos were also used. Making comparisons and asking “practical” questions to build theory were the major methods of analysis in this project.⁴² Building sensitivity, defined by Corbin and Strauss as “insight, being tuned in to, being able to pick up on relevant issues, events, and happenings in the data,” were also an important part of the qualitative analysis process.

1. Coding and Analysis

A hybrid approach was taken in coding the interviews. This hybrid model is part way between a responsive interview formal coding schema and grounded theory models in that not every term was coded, but only concepts and themes that were closely related to the research question were selected.⁴³ The literature was reviewed in order to acquire understanding of the themes and concepts that should be coded.⁴⁴ A grounded theory approach was used where the themes and concepts were allowed to emerge from the data. Line-by-line open coding, the breaking apart of data in order to generate additional concepts and themes that may not have appeared in the literature, was performed.⁴⁵ The researcher gathered data and analyzed it concurrently. This also allows the development of “sensitivity,” whereby the researcher by “alternating processes of data collection

⁴¹ Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research*, 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 198.

⁴² Ibid., 72 - 73.

⁴³ Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data*, 2nd ed. (Sage Publications, Thousand Oaks, CA, 2005), 223.

⁴⁴ Ibid., 221.

⁴⁵ Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research*, 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 198.

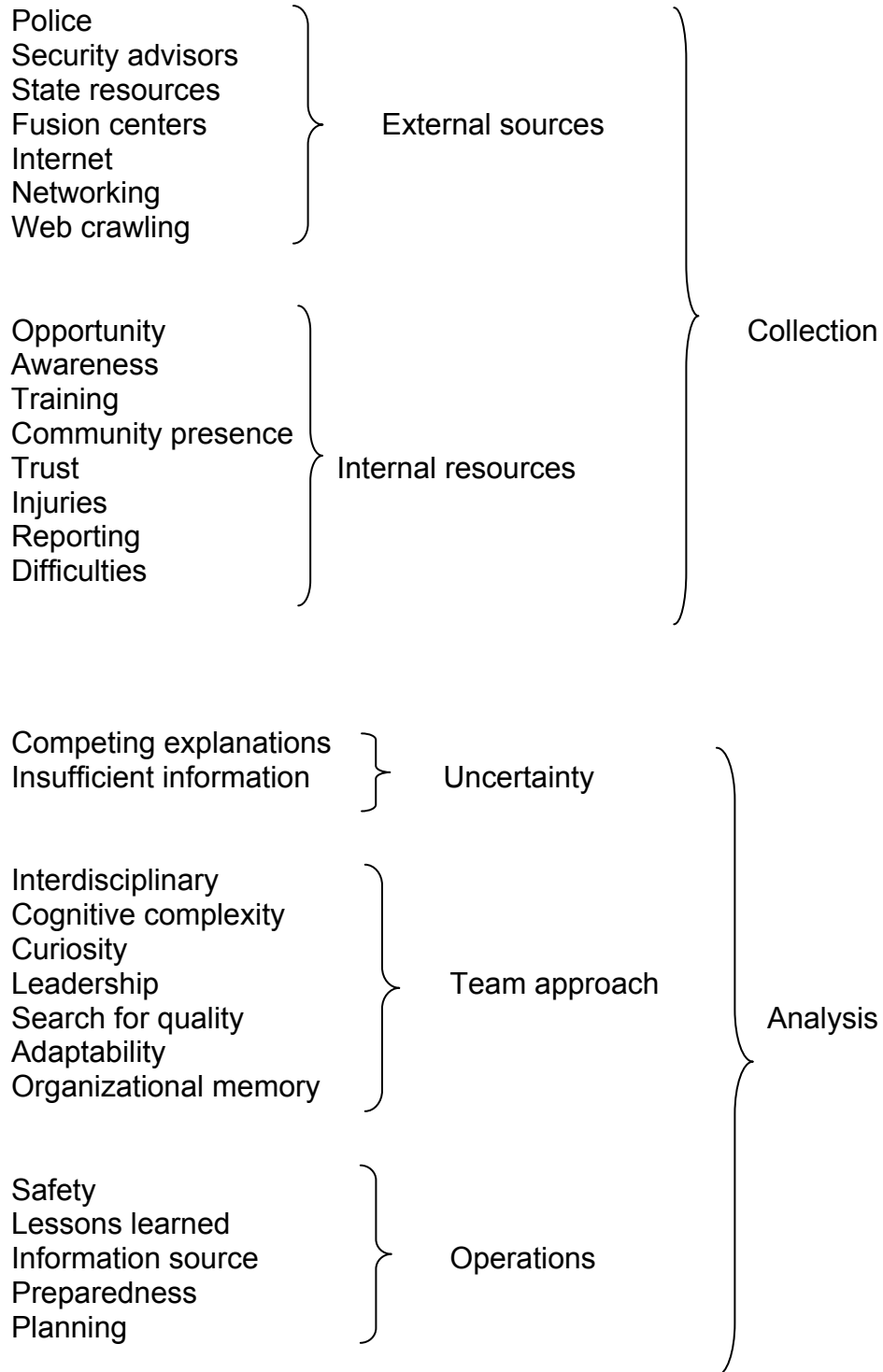
and analysis, meanings and significance of data, often illusive at first, becomes clearer and the researcher begins to see the issues and problems from the perspective of the participants.”⁴⁶

Data acquired from the interview transcripts, e-mails, and the researcher’s field notes were coded and reviewed until coherent patterns began to emerge. This analysis was performed by “constant comparison.” In this methodology, “incidents found to be conceptually similar are grouped together under a higher-level descriptive.”⁴⁷ Constant comparison was necessary because it allowed the researcher to distinguish the various themes and concepts. Data was broken down into “informant codes,” which were aggregated into higher order analytic codes and finally second order codes, and more general categories and themes, were induced (See Figure 1). Theoretical saturation was not reached due to time constraints mandated by the program.

⁴⁶ Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research*, 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 32.

⁴⁷ Ibid., 73.

<u>Interviewee Codes</u>	<u>Analytic Codes</u>	<u>Aggregated Second Order Categories</u>
Inform Reduce risks Prepare	} Purpose	} Intelligence
Secret Sharing Unclassified	} Open Source	
Artificial Useful	} Intelligence Cycle	
Discussion Determining	} Brainstorming	} Requirements
Ignorance Analytical autonomy	} Freedom	
Mission orientated Actionable Timeliness Implications Situational awareness Cyber threats Infrastructure	} Guidelines	



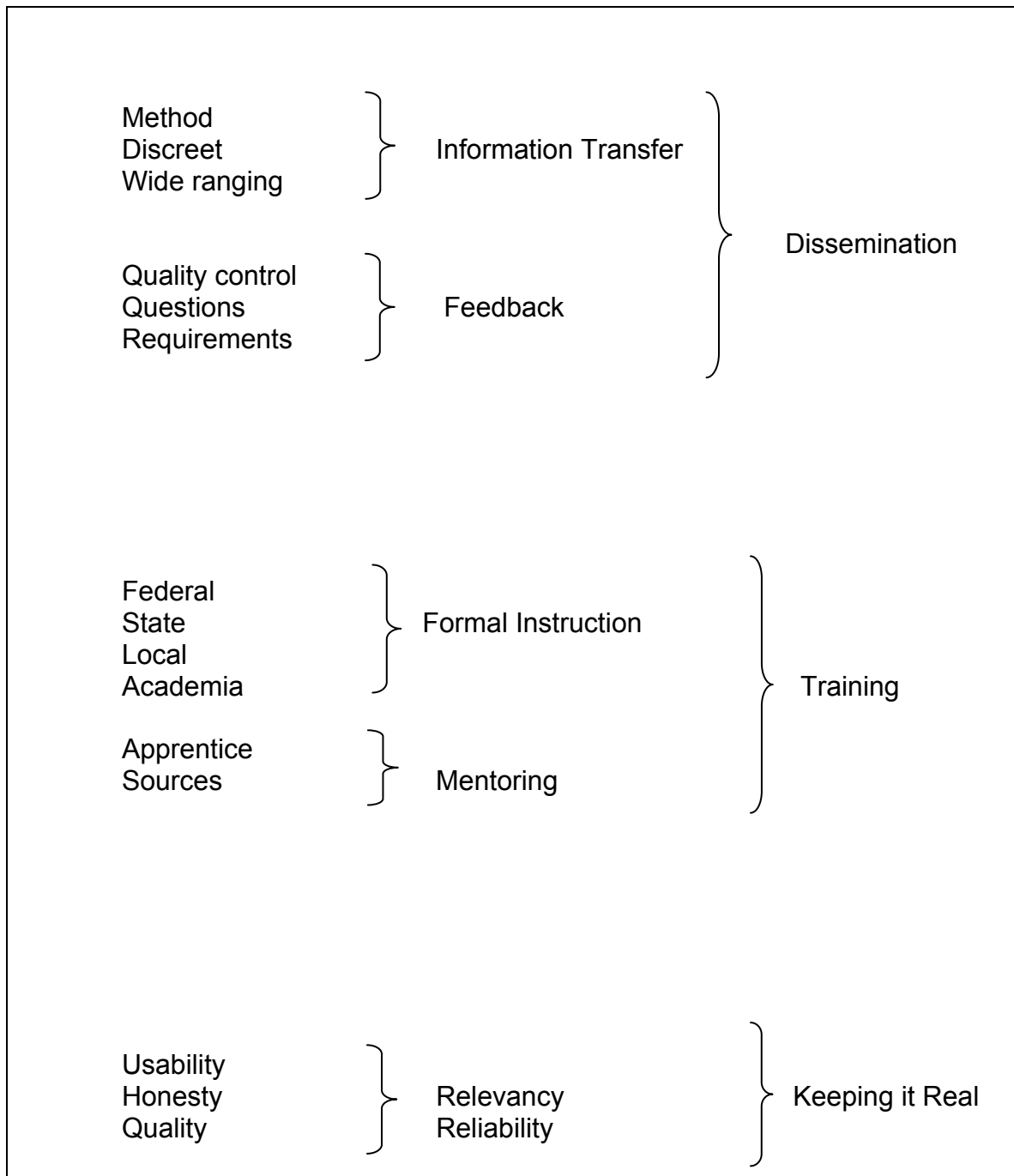


Figure 1. Emergent Analytical Codes and Categories

2. Writing

The data from the interviews was interpreted by the researcher in light of the needs of the fire service without getting too far from the idea as a

experiences of the subject matter experts. Most importantly, the researcher sought to avoid a theoretical approach and instead attempted to provide useable information arising out of the first hand experience of the involved intelligence professionals. It is the researcher's fondest hope that this thesis is actionable by the fire service in understanding and using intelligence. In writing this thesis, the advice of Rubin and Rubin has been followed, which is to use extensive quotations from the interviews in order to make the interviewees real.⁴⁸

⁴⁸ Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data*, 2nd ed. (Sage Publications, Thousand Oaks, CA, 2005), 252.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DATA ANALYSIS

A. INTELLIGENCE

1. Purpose

What is the purpose of forming a fire department intelligence unit? The answer is simple; to protect the members of a department and the community they serve. Francis Bacon, the 17th century English philosopher, once said that knowledge is power. The fire service has always known this to be true. Firefighters learn hydraulics, building construction, emergency medicine, line placement, hazmat, and so many other topics because this knowledge gives them the power to do their jobs properly. “Good information allows for good decision-making. Bad information or a lack of information always results in poor decision-making.”⁴⁹ An intelligence unit has the same function, except in the field of terrorism. When asked what he saw as the purpose of a fire department intelligence unit, Fred Burton replied, “Well, you’re going to make your department better educated, better informed, better trained, more cognoscente of the life safety threats, the risks you run. With an intelligence shop, you are going to make your fire fighters smarter and your command staff better informed. You, at the end of the day, may even save lives by having analytical assessments done on your first due response areas.”⁵⁰ Later in the interview, he explained it’s all about, “life safety, meaning we are going to create an intelligence analytical capacity within (the department) in order to save lives, period. We’re going to serve the civilian population better because we’re going to do intelligence-led fire fighting versus reactive fire fighting.”⁵¹ This is the ultimate purpose of any fire department intelligence unit.

⁴⁹ “Fire Department Intelligence Officer,” *FDSOA Safety-Gram* 15 (February 2007): 1.

⁵⁰ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

⁵¹ *Ibid.*

Of course, having a fire department intelligence unit does not guarantee safety and there are costs to having such a program. So, why do it? Speaking of terrorism, George Friedman stated, "Most of it won't come here (the United States). And some of it may come here (and) we will not be prepared for it. What you're trying to do is cut the odds down."⁵² Intelligence is not a panacea. It is not foolproof; however, intelligence has a real value, perhaps life saving value, to the local fire department and every department from the largest municipal agency to the smallest volunteer organization should have an intelligence unit or at least an intelligence officer who looks at terrorism and says how might this affect my department; how might this affect my locale? "The point is that good intelligence is cheap in a sense that it doesn't have a tremendous amount of bells and whistles."⁵³

Fire departments should be thinking about and planning their response to a potential terrorist attack. They owe it to themselves and to their communities. Unfortunately, terrorism is going to be around for a long time. The intelligence unit or officer should also be used in strategic and tactical planning as an information source. For instance, hotels have become a major terrorist target around the world. They are a soft target that is easy target. There have been major terrorist attacks against hotels in Amman, Jordan, Islamabad, Pakistan, and Mumbai, India. The attacks have caused craters in the street interfering with the positioning of apparatus, mass casualties, gas leaks, fires, and structural collapse. What are your department's plans if an attack should happen in your city, town, or village? Developing plans to respond to such a situation at a hotel or other soft targets in your response area is one of the times brainstorming and the involvement of several chief officers may be required; however, the intelligence office should be able to find a lot of information on these attacks and the damage that they cause. This will help a department keep its planning realistic. How many hotels or other soft targets exist in your geographic area?

⁵² George Friedman, interview by author, field notes, Austin, Texas, November 19, 2008.

⁵³ Ibid.

Do you have floor plans, and satellite maps? Does your department know what auxiliary fire protection equipment is present? What is the back-up plan if these systems are rendered inoperable? All these items can be collected by the intelligence office for planning purposes.

2. Open Source Intelligence

Though secret and top secret intelligence may, at first, seem to be the most attractive, it is not the most useful form of intelligence for the fire service. Since most fire department personnel do not have security clearances and the process of getting clearances is long and cumbersome, the most useful type of intelligence information is open source intelligence (OSINT), especially since most fire departments will want to disseminate received intelligence information to all of its members. "Due to its unclassified nature, OSINT can be shared extensively without compromising national security."⁵⁴ Information that cannot be shared with the units in the field may have limited value.

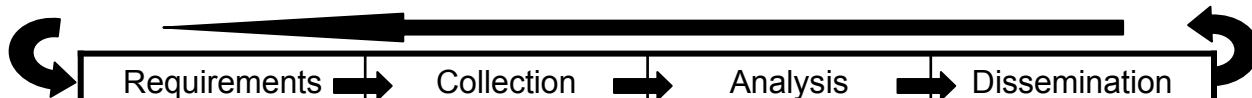
The interviewees were almost unanimous in their belief that secret and top secret intelligence was not required for the fire service. However, even unclassified open source intelligence may create difficulties for the average fire department because most are not currently equipped to handle it. Assuming that the local fire department is receiving intelligence, the flow of information coming from the Federal government and local fusion centers may be massive and requires additional processing by fire departments to exploit this intelligence properly. This is because, currently, much of the information flow is not specific or useful to the fire service. Much of it tends to be for use by the law enforcement community. Hence, a local fire department needs to put an analytical mechanism in place to separate out what is useful from this information flow, the signal-to-noise problem. Therefore, the local fire department needs

⁵⁴ Eliot Jardines, *Using Open Source Information Effectively: Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security of the House of Representatives June 21, 2005* (Washington, D.C.: U.S. Government Printing Office, 2007), 13.

specifically trained personnel and systems to accomplish this processing and analysis. Most fire departments do not have the systems or the personnel in place properly to utilize OSINT, nor do they have the experience to build such systems. The interviewees gave of their time and the benefit of their expertise in order to help the fire service build those systems. The following chapters are meant to assist a fire department that sees the value of good intelligence and situational awareness to begin to build the required structures and expertise.

3. The Intelligence Cycle

Even though the intelligence cycle is somewhat of an artificial construct, it has been used in this thesis because it provides a useful framework in which to discuss intelligence. All of the steps of the intelligence cycle may be going on at the same time; some steps may not be as clear-cut as they are made out to be in the literature. It is important to remember that the intelligence cycle is iterative. The products a unit develops may lead to other questions and then to other products. Nevertheless, an intelligence unit needs to give some thought about each of these steps in order to produce a worthwhile and useable product. In addition, it will allow personnel in a fire department intelligence unit to communicate using a common language with intelligence analysts in other fields. This intelligence cycle architecture was certainly helpful in the interviews with the subject matter experts. Figure 2 presents a descriptive précis of these steps, including some illustrative quotes.



	Requirements	Collection	Analysis	Dissemination
Description	Requirements attempt to define the needs of the consumers of intelligence within a department. In other words, an intelligence unit tries to identify and prioritize what intelligence will assist a particular department in the discharge its duties.	Collection is the process of obtaining the information needed to fulfill the requirements set by a department or information assembled in those areas that the intelligence unit thinks is important. Collection may come from outside or from within a fire department.	Analysis is the process by which raw information is developed into intelligence. This happens when analysts add their skill and expertise to the information. They add depth and perspective to the raw data. Analysis tries to answer the question, "What does this fact or incident mean to this fire department."	Dissemination is the delivery of intelligence products too those who need it. Part of the dissemination process is the request for feedback. Feedback helps with quality control and allows consumers to ask questions. These questions may become requirements for which the intelligence unit begins to collect information.
Quotes	<p>"Sit down with a few people and brainstorm."</p> <p>"What you need to do is look for is the next way a terrorist might hit you."</p> <p>"So, what you are trying to do with an analytical shop is not so much approaching it from a requirement basis, but you are trying to inform your . . . chain of command on issues that they have no knowledge of."</p> <p>"There will be some lessons learned from what happened in places like Bombay, what happened in Spain."</p> <p>"I would advocate simultaneously talking to all levels (of a department) to determine what their needs are."</p> <p>"I think you've got a really tricky problem because . . . the firefighting challenges are not the same everywhere."</p>	<p>"At the outset it's probably better to just plug in to the wealth of people at the federal and state level who are already collecting information."</p> <p>"You have to know what is happening in Amsterdam; you know the latest techniques that have been used in Cairo. You must maintain a constant global watch on technology."</p> <p>"Firefighters see a whole lot of things that are or could be reportable and I think they need the method or the means to get that to the right people."</p> <p>The US is not going to be the place where attacks are pioneered. They are pioneered in (other countries); they are field tested there. So you need to be aware of evolving trends before hand."</p>	<p>"I think at some point you have to have a human analyst who knows fire . . . and maybe teamed up with someone who knows the intelligence industry."</p> <p>"If you box people in with too many rules, and regulations, and standards then you lose free expression, you lose free thinking, and there is the innovative thinking."</p> <p>"You have three or four smart guys . . . who love sitting at computer screens 12 hours a day and discerning patterns."</p> <p>"Curiosity would be a major quality, curiosity, determination."</p> <p>"Your intelligence division, for example, could provide you with some very concise warnings and indicators."</p> <p>"Your threat to mid-town is different than Wall Street, and it's different from Brooklyn and it's different than Harlem."</p>	<p>"So, I would try to do it through the existing (mechanisms), you don't want to necessarily set up a brand new information sharing process."</p> <p>"So, yes, try(ing) to penetrate and infiltrate the existing process is probably a good initial approach at least."</p> <p>"Have a method for disseminating it (intelligence) not only to the fire department but to the police as well so that they can be alerted to it and also put it into the (department) training site."</p> <p>"For each article we put up on our web site anyone reading that can respond and ask a question, make a statement, whatever, and once they hit the send button it comes to our customer service team who are not the experts, but they will immediately pass it off to the author or someone else who knows about the subject matter."</p>

Figure 2. Stages of the Intelligence Cycle: Description and Representative Quotes

B. REQUIREMENTS

The most important step in the intelligence cycle is to define what a particular organization or policy maker needs to know. No other step in the cycle can be performed until these needs are established and all the work that might be put into the subsequent steps of the intelligence process is wasted if policy makers and the members of a department get junk information because no well thought-out intelligence needs have been established. Setting requirements is not only the most important issue a department needs to determine, but also generally, the most difficult one. It is an even more difficult question for the fire service since intelligence requirements need to be defined on a local level and the local fire department often lacks the experience with intelligence to tackle this task. As John McCreary said, "I think you've got a really very tricky problem because . . . the firefighting challenges are not the same everywhere."⁵⁵ Yet, the question of defining intelligence requirements is critical and needs to be carefully considered by the local department.

The intelligence professionals interviewed had several ideas on how a local fire department should begin to define its intelligence requirements. Not all of the interviewees agreed with each other on how they would perform this function; however, almost all stressed its importance. On the other hand, the ideas they tendered were not necessarily mutually exclusive; a local department may wish to try a blended approach, using several ideas below to establish its requirements. Departments should not be afraid to change its requirements creation process if the existing system is not working as well as it should. Additionally, a department can and must update its requirements as the local environment evolves.

1. Brainstorming

Brainstorming is an important part of this process. One of the interviewees said that if he were hired to start an intelligence office for a fire

⁵⁵ John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

department he would “sit down with a few people and brainstorm.”⁵⁶ As an outsider coming into the fire service, he would take “some time to observe, and listen, and talk to the people who do the work, not only the firefighters on the line but the investigators;” “this is pretty much step one.”⁵⁷ Mr. Johnson points out that each level of command has their own need and he advocates, “Simultaneously talking to all of these levels to determine what their needs are.”⁵⁸ Only then, can one connect the thoughts and determine where information can be effective in helping a department fulfill its role in protecting a community against terrorism.⁵⁹ This is good advice for anyone tasked with deciding a department’s intelligence requirements, even those experienced in the fire service.

2. Freedom

Another school of thought says, “in essence, they (the local fire department) don’t know what they don’t know, meaning how do you create a requirement based upon an intelligence gap?”⁶⁰ In other words, it is very difficult for a department to set its requirements, since “it doesn’t know what it doesn’t know.” Fred Burton stated that a department might know where every hydrant is on a street, and send someone out to test them and make notifications if one is down, “but you may not be aware of the real threat that lies on that street.”⁶¹ How does one solve this problem? The answer is pick good analysts and allow them the freedom to discover the real threats. These analysts pick their issues without undue interference from the higher echelons of a department. “What you’re doing with an analytical shop is not so much approaching it from a requirements based (system), but trying to inform your managers and your

⁵⁶ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

⁵⁷ Ibid.

⁵⁸ Ibid.

⁵⁹ Ibid.

⁶⁰ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

⁶¹ Ibid.

bosses and your chain of command on issues that they have no knowledge of whatsoever.”⁶² In other words, rather than trying to set up formal requirements, a department is really depending on its analysts to come up with answers to questions that nobody has thought of as yet.

These two systems are not necessarily in opposition to each other. A department could establish some formal requirements for its analytical unit to handle. These would be established through brainstorming and discussion with each level of a department in order to see what intelligence is necessary to respond to terrorism as safely as is possible. Yet at the same time, the analysts could be given the freedom to answer questions that nobody has asked, but that the analytical team thinks is important. This is because a department may need “to know those things that somebody hasn’t sat around and thought of” yet.⁶³

The alternative to locally defining requirements is to allow other agencies to give whatever intelligence they deem relevant and hope that the fire department receives the right information. This school of thought says that since fire departments may not have their own analysts, they “should be receiving properly analyzed and corroborated information, unless that information relates to an imminent incident or threat.”⁶⁴ On the other hand, locally specific, well thought-out intelligence requirements would also help the Department of Homeland Security (DHS) and other federal entities fulfill their missions within the National Information Sharing Strategy, while not overwhelming the local fire service with large quantities of information of limited relevancy.

3. Guidelines

Below are some additional ideas on helping a local department establish what it needs to know. First, any intelligence requirement produced by the fire service must support its core mission. The core mission of any fire department is

⁶² Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

⁶³ Ibid.

⁶⁴ Fire Service Intelligence Enterprise (FSIE), *Progress Report 1* (December 28, 2008), I-2.

protecting life and secondarily protecting property in their community; these are the *raison d'être* of the fire service. For instance, the “the core mission of the FDNY is life safety.”⁶⁵ If the proposed requirements do not directly support a department’s mandate to protect life and property, they are faulty. For instance, knowing the strategic balance between the United States and a resurgent Russia may be important, even critical, to the national security of the United States, but such intelligence is probably not necessary for the fire service to protect the citizens of its local community. On the other hand, a department may want to know about the latest terrorist attacks in India.

Further, intelligence is not primarily an intellectual exercise, meaning that the information requested should not be “interesting,” but “useful.” Therefore, the second standard for a fire service intelligence requirement is that it should be useable. Lowenthal makes the point that policy makers “seek intelligence that is actionable intelligence, that is, intelligence with which they can do something.”⁶⁶ This desire for actionable intelligence is just as true for the fire service. Hence, intelligence that has no practical application is of little value to any department.

The third requirement for intelligence is timeliness. Intelligence must not be received after it is no longer useful. The timing of intelligence may be broken into two broad categories. Long-term intelligence should be more in depth and looks at what may happen in one month to several years. Long-term intelligence is also known as strategic and operational level intelligence. This type of intelligence is useful to the fire service because it allows for longer term planning for equipment purchases; it allows time to create and implement necessary training, and permits drills to be carried out. Additionally, departments can craft better standard operating procedures if it has an idea of how terrorist groups may act. Short-term intelligence involves warnings of an imminent attack. Short-term or tactical intelligence may cover the period of one day or less to several weeks.

⁶⁵ Fire Service Intelligence Enterprise (FSIE), *Progress Report 1* (December 28, 2008), 13.

⁶⁶ Mark M. Lowenthal, *Intelligence from Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006), 234.

In this period, there may be little occasion for a department to prepare thoroughly for the attack. However, staffing levels may be increased and curtailment of nonessential fire service activities initiated.⁶⁷

Given these provisos, what kinds of intelligence does the local fire service need? The answer is simple; a local fire department needs good situational awareness. The department needs to know what is going on in the world of terrorism. What is happening strategically and tactically with terrorist groups? This information may come from other countries or it may cover what is happening in the United States. Most importantly, what is the possibility of an attack on their local community? How will it most likely happen? Are there changes in terrorist tactics that the fire service should know about? Are there signs or warnings of imminent attack? What types of improvised explosive devices (IEDs) are being used around the world? How are these IEDs being used? For instance, George Friedman stated, "What you need to look for is the next way a terrorist might hit you. Okay so cell phone detonated bombs, well they are old hat now, but coming along is some other really nasty thing."⁶⁸ This is what the local fire service needs someone to be looking for. Is there an increasing amount of secondary attacks? Have there been attacks specifically against fire departments? In other words, what is going to hurt your department and the people you serve?

Attacks from around the world need to be examined in light of a local fire department's community. A department needs to look at the implications of foreign and domestic attacks with an eye to how that particular department operates. Attacks that take place in the United States will probably have been tested in other parts of the world. "As part of this effort," a department should realize "there will be some lessons learned from what is happening in places like Bombay, and what happened in Spain."⁶⁹

⁶⁷ Fire Service Intelligence Enterprise (FSIE), *Progress Report 1* (December 28, 2008), I-2.

⁶⁸ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

⁶⁹ John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

Weapons of mass destruction are another area of concern. Though they may have a low probability of use, they have the potential for high casualties as well as potential for extensive property and economic damage to a locale. Any long or short-term intelligence from federal or state agencies can supply may help departments prevent, prepare for, or mitigate such an attack.

Cyber attacks, though they may not seem like a fire service issue, may adversely affect the fire department of a community. Many fire departments dispatch their units by computer assisted dispatch systems. Any damage to those systems would force a return to manual dispatch systems, which are more labor intensive. Departments may need to assign additional dispatchers to their communications office to prevent the collapse of dispatch operations. Additionally, many forms of cyber attack may hugely increase utilization of departmental assets. For instance, more and more elevators are being tied into centralized computer systems for operation, maintenance, and repair. A cyber attack on these computers may result in literally thousands of people being trapped in elevators and requesting fire department assistance. Cyber attacks on utilities may cause similarly widespread problems. Any intelligence that could either help departments to protect its systems or give it forewarning of targeted attacks may help it prepare to respond.

Another intelligence requirement is threats to infrastructure. This intelligence should not be limited to a particular city or town because most locations are dependent on such things as water and electricity from outside its own borders. This information may allow a department to do contingency planning on how it will operate if it lost the use of a specific infrastructure. One of the most important things a department needs to know about is threats to their water supply.⁷⁰ Firefighting activities generally come to an end without water.

In summary, although some interviewees distrusted formal requirements, an example list of fire service intelligence requirements could be the following.

⁷⁰ John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

- Situational awareness and terrorist threats
- Improvised explosive devices
- Weapons of mass destruction
- Cyber attacks
- Threats to infrastructure

C. COLLECTION

Does a fire department need to go out and begin its own raw collection? In other words, does the fire service need to hire and run agents on the street? The answer, of course, is no; that is not what this thesis is suggesting. It would be both cost prohibitive and inappropriate to attempt this kind of collection. In addition to the potential legal difficulties, it would be beyond the scope of the fire service's mission to attempt to do so. So, then, how does a fire department intelligence unit find information in order to fulfill its mission? It might be less of a problem than most think. Indeed, the real problem is not so much that there is not enough information out there; the problem is that there is too much data. The difficulty is that "there is too much information out there to make sense of it logically because today we are inundated with information."⁷¹

1. External Sources

The information to collect is that which supports the fire service's mission to protect life and property in its local community. Therefore, a good place to start is to have an intelligence unit or intelligence officer liaison with the local police department. The local police usually has a finger on the pulse of the local community. There may be state and local police in a particular area and a fire department should make contact with all of them. In addition to being able to supply information that may be of use to a department, the personnel involved become familiar to each other. Then if an emergency occurs, the agencies are not strangers but have, ideally, already built a level of trust with each other. Pat

⁷¹ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

Miller stated, "Because they (the police department) are tied into so many different systems that the fire department isn't, that's where you need to start."⁷²

All appendices are restricted.

The next set of people to make contact with is the U.S. Department of Homeland Security's Protective Security Advisors (see Appendix A). "In 2004, the Risk Management Division (RMD) Field Operations Branch (FOB), established the Protective Security Advisor (PSA) Program, deploying a cadre of 68 critical infrastructure security specialists, with an average of 20 years of law enforcement, military, and anti-terrorism experience, permanently assigned to 60 metropolitan areas designated as PSA districts across the United States."⁷³ One of the areas where a fire department's intelligence unit can be helpful to its department is in the area of critical infrastructure in a local community. Where is it? What are their dangers? Would this facility create any special difficulties in firefighting or hazmat response if it were involved in a terrorist attack or other disaster? The intelligence unit should be asking these questions. Pre-operational planning should result from this research. The local PSA is a valuable source of information and can make introductions where necessary to local critical infrastructure operators. This is significant because local infrastructure operators are experts with unique insights into their facilities; they are an important resource. Additionally, PSAs act as a line of communication between the local community and the Department of Homeland Security in the area of potential threats, and they can help with exercise design in their geographical area. The intelligence unit can use this assistance if it is called upon to set up drills for its department.

⁷² Pat Miller, interview by author, field notes, South Bend, Indiana, November 22, 2008.

⁷³ "Protective Security Advisor Program Overview," http://www.cops.usdoj.gov/files/ric/CDROMs/PlanningSecurity/modules/11/Module11_ProtectiveSecurityAdvisor.pdf (accessed January 16, 2009).

Additionally many states have homeland security departments. A fire department intelligence unit should make contact with them and see what services these agencies might have available. "The homeland security (agencies) at the state level . . . have a broader view of things and they are not just law enforcement, they're also first responder."⁷⁴

Next, the intelligence officer of units should make contact with the local or regional fusion center (see Appendix B). They may well be a great source of information. However, the unit should not become overly dependent on the fusion center alone. There are several problems with the fusion centers. One is that their future is uncertain. In addition, the quality and scope of their work is uneven. There is a saying that goes, "You've seen one fusion center, you've seen one fusion center." In other words, each fusion center is unique both in terms of what it fuses and in terms of how well it does it. The other problem is that fusion centers tend, with few exceptions, to be law enforcement focused. "And everybody else including the fire department is kind of a second team. If they participate they do, but we (the fusion centers) don't care if they don't."⁷⁵ Some of the interviewees also questioned the usefulness of many of the products the fusion centers generate to emergency personnel on the street. Others thought they might be useful. "Fusion centers can be useful provided everyone shares information. Across the country, you will find various opinions as to the usefulness due to turf issues. I see duplicate efforts in a lot of places."⁷⁶ Due to these limitations, a fusion center should not be a department's only source of information.

This is not to say that one should not contact and use the local fusion center. An analysis unit absolutely should. Indeed, one suggested alternative to a fire department having its own intelligence unit is to place firefighters in the regional fusion center as analysts. "A couple of people who have a firefighting

⁷⁴ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

⁷⁵ Pat Miller, interview by author, field notes, South Bend, Indiana, November 22, 2008.

⁷⁶ Fred Burton, e-mail message to author, January 19, 2009.

background” could “establish a firefighting intelligence desk or something at the fusion center and their job would be to look through all the flows of information coming in and pull out the relevant things to the firefighters, to the first responders, and the allied disciplines.”⁷⁷ Some fusion centers are doing this. However, that still leaves the need for the local fire department intelligence unit to look at the materials posted by their fusion center and see how it applies to their department, with its particular infrastructure, and its particular policies and procedures.

There is a wealth of information and processed intelligence available on the internet (Appendix C). Most of these web sites require that a department apply for access to them. The information they contain is voluminous and covers just about every aspect of terrorism. For instance, the Overseas Advisory Council (OSAC) does good analysis of what is happening around the world and creates excellent PowerPoint presentations on major terrorist attacks around the world. “You have to know what is happening in Amsterdam; you have to know the latest techniques being used in Cairo. You must maintain a constant global watch on technology.”⁷⁸ A department needs to “watch the technologies that are evolving in other parts of the world. The U. S. is not going to be the place where attacks are pioneered. They are pioneered in (other countries) – they are field tested there. So you need to be aware of evolving trends beforehand.”⁷⁹ This knowledge should support one’s training for a response to a terrorist incident. Others like the Universal Adversary Portal contain information on terrorist groups and information that is helpful in exercise planning. This includes terrorist groups that operate within the United States. This is because a fire department must also look within the country at terrorist trends as well. “9/11 showed us you

⁷⁷ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

⁷⁸ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

⁷⁹ Ibid.

can't just focus on overseas; a focus only on overseas doesn't necessarily guarantee security."⁸⁰ Still others sites contain information on such topics as critical infrastructure and weapons of mass destruction.

The Open Source Center (<https://www.opensource.gov/>) site is especially helpful because it has a subscription service that will e-mail the intelligence unit materials that they request. This is an example of a pull site; the user pulls what they think useful to their organization.⁸¹ A fire department analyst should think about the subscriptions they might find useful. Certainly, words such as "fire department," "arson," "fire bombings," "improvised incendiary devices," and "terrorism" should be included in the subscription. Additionally, an analysis unit should request that the Open Source Center send them anything that mentions the name of their state or locality. Two entities are especially useful to the fire service because they are more fire related than most sites. One is the Emergency Management and Response Information Sharing and Analysis Center site (EMR-ISAC), which is run by the U.S. Fire Administration. This site will send e-mails and infograms with emergency sector specific intelligence and information. Chief Officers may receive Sensitive Compartment Notices, which are "For Official Use Only."⁸² The other is Watch Line, a product of the Fire Department of the City of New York's Center for Terrorism and Disaster Preparedness. The Center produces it weekly and is a good vehicle for fire departments that are trying to improve their situational awareness. Almost all of the information in Watch Line is useful to the fire service.

The members of the intelligence and analysis unit should always be making connections. Every time members of the unit go for training, every time its members go to a conference, talk to other people at the training event, the speakers, and the instructors; make contacts. Get a business card if possible;

⁸⁰ John McCreary, interview by author, field notes, Washington, D.C., November 25, 2008.

⁸¹ Mark Johnson, interview by author, field notes, Washington, D.C., November 4, 2008.

⁸² Charles Werner, "Progress Report: Information, Intelligence for the Fire Service," Firehouse 29 (December 2004), 40.

file the card. Jot a few notes about the person or agency on the back of the card. Do not just do this for other fire departments. A department might want to do this with federal and police agencies, infrastructure operators, the radiation hygienist at the local hospital. The unit must use its imagination. Get anyone and everyone's card. You never know when that contact might help your department. Thus, if a question arises or something happens in another locale, the intelligence unit can contact that person and get the straight story. It is suggested that this be done even if it is necessary to make contact with another fire department in another state. On the flip side, have a business card available and give it out. Help where possible. Networking can be invaluable to an intelligence unit.

Lastly, some of the interviewees suggested that the intelligence unit could collect raw material right off of the internet. For instance, Mark Johnson gave an example, "I'll bet if you go on YouTube today and type in, how to set a fire using whatever or how to build a bomb, you are going to find videos on there that tell you that and some could be . . . in the (department's) region or city."⁸³ A contractor can set up a web crawler to look for these kinds of materials in a particular area or nationwide. The intelligence unit would need to review these materials to see if they have any value. However, this level of sophistication is probably beyond the scope and abilities of most fire department analytical units.

2. Internal Resources

There is another source of information for the intelligence unit that should not be ignored. That is the members of one's own department. The 316,950 professional and 823,950 volunteer firefighters in the United States enter thousands of buildings on a daily basis.⁸⁴ Firefighting personnel enter residences, factories, warehouses and apartment buildings for fires, medical

⁸³ Mark Johnson, interview by author, transcripts, Washington, D.C., November 4, 2008.

⁸⁴ United States Fire Administration, Federal Emergency Management Agency, "Firefighters," <http://www.usfa.dhs.gov/statistics/firefighters/index.shtml> (accessed August 31, 2008).

emergencies, utility emergencies (gas, electric, water), and to accomplish building inspections. “Unlike police, firefighters and emergency medical personnel are not required to obtain a warrant to enter a building.”⁸⁵ Each of these inspections and responses is a potential opportunity to gather intelligence on terrorists who may be operating within the local community. George Friedman of Stratfor stated, “I regard firemen not policemen as the first line of intelligence across the board.”⁸⁶ For instance in April 2005, in the course of a routine building inspection in Brooklyn New York, members of the F.D.N.Y. found more than 200 airbags in the basement of a food market that also had newspaper clippings about Osama bin Laden and beheadings in Iraq covering the walls.⁸⁷ Now, purportedly this incident was not related to terrorism; however, in addition to the obvious clippings, firefighters realized that airbags contain an explosive charge, sodium azide, which could be used by terrorists.

The important point here is that information received by the fire service and disseminated by the local department’s intelligence unit increases its situational awareness, thereby, increasing its ability to recognize terrorist activity. In addition, there may also be times when federal or local police agencies have specific things they desire a local fire department to be looking out for in the course of its normal duties. Firefighters and EMS personnel must have a clear reporting mechanism for any information collected. The department’s intelligence unit or intelligence officer is the natural choice for this liaison function.

The intelligence unit also needs to work with the department’s training division in order to instruct firefighters on what they should look for or perhaps the unit needs to do the training directly. “Firefighter’s can be plugged into the training regime and you (the intelligence unit) can do annual refreshers, you can do quarterly updates, what’s new and overseas bombing overseas and other

⁸⁵ Richard Blatus, *Altering the Mission Statement: The Training of Firefighters as Intelligence Gatherers* (Master’s Thesis, Naval Postgraduate School, 2008), 5.

⁸⁶ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

⁸⁷ Rich Calder and Murray Weiss, “Stash ‘Bagged’ at Market,” *New York Post*, April 27, 2005.

events. You (the intelligence unit) may see trends and you have got to communicate with the people . . . ”⁸⁸ A firefighter cannot collect information if he or she does not know what to seek.

Another aspect of a fire department’s collection is human intelligence . . . Again, running agents and informants on the street is not what is being recommended here. What is recommended is that firefighters be trained to report what they hear on the street if it involves potential terrorist activity. George Friedman commented that if he were in charge of a fire department intelligence unit, “I would create . . . a human intelligence network. And for me a fire department is superbly located. It’s in the community, it’s in every community. It’s a non-threatening entity and your people (firefighters) have constant daily interactions with the community including stakeholders in the community, which would not just be gang members, (but) people who own stores and so on.”⁸⁹ The difference here is one of actively running an intelligence operation versus a firefighter knowing enough to report what they hear passively.

People might well be willing to talk to firefighters who are not willing to talk to the police. The community should know that they can talk to firefighters if they suspect terrorism. “The cops are feared. I’m afraid of them. Firemen are benign. They’re the people who come to your house when you’ve had a heart attack. They’re the people who will save your kids when they have done something really stupid climbing up somewhere.”⁹⁰ This is not to say that this trust should be abused; however, firefighters should be trained to listen. “Your guys are in neighborhoods . . . where somebody might tell you, ‘You know don’t tell anybody but my cousin is kind of insane and I don’t know what he has in his bedroom, but it smells bad.’”⁹¹ Firefighters should be trained and motivated to report something like this.

⁸⁸ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

⁸⁹ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

⁹⁰ Ibid.

⁹¹ Ibid.

A department's emergency medical response personnel should be trained as well. They might see injuries that are unusual. If terrorists are using chemicals to produce explosives or chemical warfare agents and something goes wrong, medical response personnel should be trained to notice the atypical injury. Does the story behind the injury match the injury; is the injury really weird? One interviewee asked, "Where does the (report of) interesting wounds, the burns that don't make sense, acid burns that don't make sense, shrapnel wounds in the leg" get directed to? "Because that's how you are going to find a terrorist cell. Someone is going to do something boneheaded with one of his systems, cause a fire, cause a wound to himself and so on."⁹²

Multiple interviewees emphasized the importance of having a clear reporting mechanism. It might be as simple as putting a poster on the wall of the firehouse with a telephone number and most importantly someone on the other end who can answer questions or take the information.⁹³ The success of a department's firefighters serving as extra eyes and ears will only be successful if the local department "establishes a procedure and a format where firefighters would be able to know what to look for and how to report it."⁹⁴ Some cities have such a system in place. Again, the intelligence unit is the natural point of contact for these suspicious activity reports, especially since it might be able to fit the report within the larger context of what is occurring with terrorism in the region and the world. The intelligence unit, by the contacts they have previously made, should know who to pass this information onto in the local police and Federal Bureau of Investigation.

Several of the interviewees stressed the need for the system to be simple and have a reward system in place. This is not to suggest cash rewards or the like; however, "they (department personnel) need to know that what they are

⁹² George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

⁹³ Ibid.

⁹⁴ Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

doing matters.”⁹⁵ Every report gets a response. Even if there is already an ongoing investigation and the fire department intelligence unit cannot reveal the specifics of a case, the reporting personnel still get an individual telephone call from the unit thanking them for the report. This tells department personnel that someone is listening, someone is responding to their report. They are not wasting their time. Failure to respond will cause the failure of this effort. If the process is not simple or firefighters never hear anything back on the reports they file, “people aren’t going to take the time or they’ll do it once and say screw this.”⁹⁶

However, this is not to say that firefighters should become intelligence agents for the federal government or police officers. This would create both constitutional and public relations problems. In November 2007, the American Civil Liberties Union attacked the FDNY for its reported “training” in intelligence gathering. The ACLU spokesperson asked “do we want people to fear the fire department as well as the police.”⁹⁷ While the question is unfair, it does contain a word of caution. The fire service must remain scrupulously within the limits of the law while still performing this vital function. Of course, a “fire department must guard against drifting into law-enforcement activities – namely, investigating crimes and apprehending criminals.”⁹⁸ Indeed, even with meticulous attention to the legal issues, there may be a political backlash to a closer relationship with police and federal intelligence agencies. Nevertheless, terrorism prevention is clearly a part of the fire service’s life safety mandate.

There is another downside to firefighters acting as intelligence collectors. There would need to be a commitment to training fire department personnel in the recognition of the signs of potential terrorist activity. This would require a

⁹⁵ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

⁹⁶ Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

⁹⁷ MSNBC, November 23, 2007, <http://www.msnbc.msn.com/id/21940968/page/2/> (accessed August 31, 2008).

⁹⁸ Kyle Dabruzzi and Daveed Gartenstein-Ross, “Firefighters’ Developing Role in Counter Terrorism,” *Policing Terrorism Report* 3 (July 2008): 2.

portion of a department's limited training time that one could argue would be better spent preparing for fires and emergencies. Nevertheless, whatever the public relations problem, and whatever the necessary commitment of resources, they must not deter the fire service from exchanging lawful information with other agencies. Such a two-way passing of information and intelligence helps the fire service to fulfill its sworn duty to protect its citizens, their fellow first responders, and themselves from a terrorist incident. Secondly, a local fire department must protect the property and economic resources of its community. The fire service's obligation to "protect life and property" supersedes any potential downside to firefighters keeping their eyes open in the course of their normal duties.

In summary, a fire department intelligence unit collects information from multiple sources. Its staff forms relationships with personnel in other agencies in support of its mission. John McCreary said of this unit, "What you guys have to do is set up a liaison core."⁹⁹ The intelligence unit should not just be sitting in an office. In addition, it uses online resources supplied by the local fusion center, the Department of Homeland Security, and federal law enforcement and intelligence agencies to find applicable material. They obtain information from the members of their own department. Collection is a function that requires imagination and adaptability. Imagination is the only limit to where and what types of information can be collected.

D. ANALYSIS

Intelligence is more than just gathered facts. An analyst is more than just a person who collects information and passes it along to someone else. The analyst or analytical team must know what is important to the people or the organization they serve. With this in mind, they collect information and add value. The value they add is their own expertise. They add depth of meaning and insight. More than just facts, they try to give an understanding of what these

⁹⁹ John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

facts could mean to their consumers. How does this individual or team help a fire department manager? Fred Burton posited, “I don’t have time to read . . . 25 different websites and six different E-mail providers a day. So, your analytical shop, your intelligence division, for example, could provide you with some very concise warning and indicators, information as to what you should be thinking about, not only from a tactical perspective, but a strategic perspective.”¹⁰⁰

1. Uncertainty

This does not imply there is only one possible explanation of what some piece of information could mean; sometimes there may be several competing explanations for a set of facts. An efficient group of analysts may explain the strongest possibilities and discuss the implications of each. Additionally, in most cases, there will be incomplete data on a particular topic. This does not mean that an analyst should not evaluate the existing information, but it does mean that they should convey the level of uncertainty. “One way to help convey uncertainty is to identify in the analysis the issues about which there is uncertainty or the intelligence that is essentially missing but which would, in the analyst’s view, either resolve the unknowns or cause him to reexamine currently held views.”¹⁰¹ How does a local fire department do all of this? Where does it obtain the requisite analytical expertise?

2. Team Approach

Almost all interviewees agreed that a team approach to analysis would be the ideal way of proceeding. Mark Johnson said, “I think at some point you have to have a human analyst who knows fire, knows the fire fighting trade, industry, and maybe teamed up with someone who knows the intelligence industry.”¹⁰²

¹⁰⁰ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹⁰¹ Mark M. Lowenthal, *Intelligence from Secrets to Policy*, 3rd ed. (Washington, D.C., CQ Press, 2006), 129.

¹⁰² Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

Pat Miller reported, “You will have to bring in someone with an intelligence background, I think, in order to do it right.”¹⁰³ Why should this be so?

Setting up interdisciplinary teams is a method that we often use to tackle tough questions. In fact, to carry it out into the ultimate . . . the National Counterterrorism Center is an interdisciplinary team. You’ve got FBI analysts up there, you’ve got CIA case officers who run spies overseas; you’ve got CIA analysts who are experts in cultural things, You’ve got DIA people who specialize in military intelligence, and you’ve got a whole host of others. So, I think that (the) principle is applicable at all levels down to a fire department. You need both, you need it all.¹⁰⁴

No one person can know it all; that is why the team approach is a good paradigm for fire service intelligence. John McCreary, an experienced intelligence professional said, “I’d have to work, sit with a knowledgeable firefighter,” I’d have “to learn from him as well as see if I can apply what you need to know.”¹⁰⁵ A team approach is ideal; however, it is not the only approach, especially if a local department does not have the resources to include an outside intelligence analyst.

How, then, does a department choose fire personnel to place into an intelligence team? What qualities does one look for in a potential analyst chosen from within a fire department? Choosing the right person is especially important for a department that may not have anyone with an intelligence background available either from within or from outside the department. The most basic answer is to choose for quality of mind. Irrespective of all other qualifications, department leadership has to look at the intellectual qualities of the individual. Obviously, the individual would also have to have an interest in the intelligence field, and certainly, expertise in certain fields such as improvised explosive devices would increase the value of an individual to a department.

¹⁰³ Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

¹⁰⁴ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

¹⁰⁵ John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

A department could make several errors in choosing an analyst, as many firefighters may not be suitable for this role. Firefighters, as a general rule, tend to be process oriented and this is not the ideal way to do intelligence. One mistake would be to take a firefighter on light duty and “make him the analyst this month. That’s a very good bureaucratic move. (However), it doesn’t help generate your intelligence products.”¹⁰⁶ Another error would be to choose analysts by rank or seniority in a department. “You could be successful at pulling it off if you had the right mindset and leadership meaning if you selected not based on seniority, not based on Vinnie’s cousin . . . throw out your seniority, throw out your rank. I’m not saying (don’t) have a boss,” but your lead analyst “may be 20 years younger than the people that ultimately would work in the unit.”¹⁰⁷ In other words, a fire department needs to make a careful choice of individuals, ones with the right qualities, irrespective of extrinsic factors.

There are many positive qualities a department should look for in personnel assigned to this enterprise.

If I was hiring someone for you, if I pulled them from the ranks I would look for qualities of curiosity, curiosity would be a major quality, curiosity, determination. They want to get to the answer but also independence of thought; they don’t necessarily go along with the crowd and I would want them to be pretty circumspect about things. I am not looking for the loner off in the corner who quietly . . . does his job but I’m also not looking for the office fly who is just constantly . . . circulating around the office yakking it up with his buddies. I am looking for someone in between, someone who’s got a pretty solid analytical head on their shoulders, but they also talk to others. They are not intimidated by rank necessarily or position; they’re looking at everything in a pretty cool-headed logical fashion but with an . . . awareness of, we are all political animals, we live in political organizations and . . . you have to follow the direction of the organization that you are working inside.¹⁰⁸

¹⁰⁶ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹⁰⁷ Ibid.

¹⁰⁸ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

Other interviewees also stressed the need to look for the individual with curiosity, and imagination; one looks for the inveterate reader. They should be the kind of people that the department gives a problem to go at it with determination; they “love brainstorming all day,” gnawing on the problem.¹⁰⁹ They should not be “boss fighters,” but also not easily cowed by rank. Lastly, they need to be self-confident in that if they were working with outside analysts they would have to be comfortable working with people who are smarter than them when they are on certain subject matter.¹¹⁰ George Friedman recommended people who “love sitting at computer screens . . . and discerning patterns.”¹¹¹

The supervisor of this unit needs to be able to guide and be patient with these personality types. He or she also needs to be able to keep the unit on track, again determination, leadership, and the ability to get the best out of team members is required. Especially in the early stages, the supervisor is going to need to assure things are getting done. The department and possibly the municipal government will be watching to see what this unit is doing. It cannot be allowed to sit around thinking great thoughts; it needs to produce useful intelligence products.

And the person that guides them doesn't necessarily have to be a professional analyst; it has to be just somebody interested in getting the mission done, a mission-oriented supervisor. And that person would say . . . , “Over the course of 90 days here, we're going to do something that has never been done before here within (this fire department). We're going to create an intelligence department to help us and to save our colleagues' lives. And the first thing we're going to look at is this. Now, how are we going to go about getting that done? And, oh, by the way, we need this done by, if this is a Monday, we need a completed project with your suggestions by Wednesday.”¹¹²

¹⁰⁹ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

¹¹⁰ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹¹¹ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

¹¹² Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

So how might a department search for the right people? First off, open the unit up to all the personnel in a department whether they are uniformed members of the department, professional staff or civilians. The idea is to have as wide a pool of applicants as possible. One interviewee said, “I would solicit requests for an extremely bright individual with good writing skills with the ability to rapidly assess and process data. That person would need to take in not only the “granular and tactical data, but recognize the importance of strategic data.”¹¹³

Have the individual write a paper on some homeland security topic that the department chooses and give them a very short time to do it. The short lead-time does two things. It shows that a person is motivated and that they are adaptable. Next, have the people the department has chosen work as a team. “I would give them projects to work on. And I would have them operate with very little direction and very guidance at first.”¹¹⁴ Again, this group is only going to be successful if they are self-motivated and adaptable.

How does a department know if the person they have placed into their intelligence unit is going to be successful? George Friedman reported that it would be known in 90 days if an individual were going to be a success in the intelligence unit. “He’s going to start giving you smart stuff. He’s going to tell you stuff you didn’t know. Okay at first, he’s only going to do it once or twice but a man that can give it to you once or twice can give you more. And if in 90 days he can’t tell you anything you didn’t know, he won’t in 2000 (days).”¹¹⁵ Therefore, a department should initially assign a member to an intelligence unit for a 90-day probationary period.

This chapter discusses the adaptability required by members of a fire department intelligence unit. Why should this be necessary? Many of those interviewed warned against “process” in analysis. In other words, having hard

¹¹³ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹¹⁴ Ibid.

¹¹⁵ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

and fast rules about how do accomplish the tasks given to an intelligence unit is counterproductive. Mr. Johnson reported, “You know, from basic training on up you’re kind of shoved inside a box and told to operate in there and with intelligence you just can’t do that . If you box people in with too many rules, and regulations, and standards then you lose free expression, you lose freethinking and . . . innovative thinking. What was (what) they said after 9/11; the intelligence failure was one of imagination.”¹¹⁶ Get the intelligence team thinking differently, thinking analytically from a strategic and tactical perspective “not thinking regulation, not thinking process.”¹¹⁷

Several of those interviewed stated that this lack of process might be uncomfortable for a local fire department ; fire departments tend to be process driven organizations. However, as George Friedman stated about not having a predictable analytical process does indeed “sometimes creates chaos. But, better chaos than disciplined failure.”¹¹⁸

So far, this chapter has discussed what to look for in a firefighter who is being considered for an analytical unit, but where does a fire department get a professional analyst to help in this effort? There are many ways. First, the department may be able to use grant money to hire an analyst. The analyst can mentor the firefighters coming into the unit. That way if the grant money runs out, the department already has a pool of trained members who can then mentor other firefighters. If this is not possible, look within the department for people who might have a military intelligence background. These individuals would not have to make a life-long commitment to the analysis unit. They could, instead, mentor other firefighters who were interested in this work. If the department is close to a military facility, talk to the commanding officer as there might be retired military intelligence people locally who might volunteer to help. Pat Miller, the Chief of Police in Ventura, California obtained analytical assistance this way. ”I

¹¹⁶ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

¹¹⁷ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹¹⁸ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

knew there were retired Navy people around here so we went out to the base and the admiral gave us some names. And we called these guys and they were more than happy to help us out. They come in and (do) . . . mostly open source stuff but they still have clearances so they are still able to see stuff and they do a great job. They collect and write brief papers.”¹¹⁹

The Association of Former Intelligence Officers (AFIO) is an educational organization of approximately 4,000 current and former intelligence professionals. The membership of the Association is spread across the United States. Leveraging the above idea, the Association was contacted by the researcher to see if they would be willing to act as a resource for fire departments that desired voluntary assistance in forming an intelligence unit. The Executive Director, Elizabeth Bancroft, graciously offered the assistance of the Association. If a fire department contacts her at (703) 790-0320, she will notify members of the Association who live in that area. If a local member of the Association is interested in helping, they can then contact the local fire department. Similarly, the Armed Forces Communications and Electronics Association (AFCEA International), an organization of 31,000, offered their assistance to fire departments that are beginning an intelligence unit. Their point of contact is Mr. Steven Ritchey, Vice President for Intelligence. Mr. Ritchey's phone number is (703) 631-613. His e-mail address is sritchey@afcea.org. If none of these resources is available in a particular locale, do without the intelligence professional; train personnel from within your department. If none of these resources is available in a particular locale, do without the intelligence professional; train personnel from within the department.

Balance is also required in an analytic unit. The smaller the group, the more critical it is to pick the right individuals. If only have three people . . . and all three are gregarious and outgoing then the unit is going to be known for, you know, these guys make all kinds of noise, they're always sending out memos,

¹¹⁹ Pat Miller, interview by author, field notes, South Bend, Indiana, November 22, 2008.

this and that, but what the hell do they know? Or on the other hand, if you hire three guys who are studious and quiet, and you know shrinking violet types then, hello, did you hire anybody.¹²⁰ Since this thesis suggests a small group of individuals, these few people will create the unit's personality. It is important, then, not only to pick the individuals with the right mental abilities and writing skills, but also to pick the right balance of individuals.

3. Operations

What is the analytical unit supposed to do for a department? How should it be helping the local fire service organization prevent, respond to, and survive a terrorist attack? A lot of information and intelligence is available from federal agencies. Still, more is available from state and local fusion centers. The analytic unit or fire department intelligence officer looks at all of this incoming information and sees how it applies to the local fire department and the neighboring community. Additionally, the unit looks at the local community and asks how would terrorism affect a response to that building, to that factory, to that piece of infrastructure? It looks at a department's standard operating procedures and asks in light of what is known of terrorism, do they need to be changed, and is it possible to make members safer. The *raison d'être* of such a unit is to work for the safety of the members of a department, their fellow first responders, and the citizens of the community they serve.

"Every significant terrorist event is reported somewhere in the world."¹²¹ Who is looking at these attacks, looking for the lessons learned, and asking what are the implications for this department? "That's the way you learn, you go from hindsight to foresight."¹²² The intelligence officer or unit attempts to predict

¹²⁰ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

¹²¹ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

¹²² John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

the results if that attack happened in their community. Within larger communities, even different neighborhoods may face different threats. Fred Burton gave an example of how this local analysis might work.

If I was trying to make this argument to the FDNY chief in New York and okay we know NYPD has this ring of steel in Wall Street or wherever it's deployed. What does that mean to me as (the department) responsible for emergency services in the area? Does this mean that thinking of this from an analytical perspective, now the bad guys won't look at this area; therefore, where would they go? Where are the other softer target areas that perhaps I need to be made aware of? In the event we do have a call for service in this "ring of steel," do I automatically dispatch . . . a full box alarm assignment versus just a first due engine company? I mean these are the kinds of things that an analytic shop could game board and give you some potential options or some alternative analysis as to other things you should be thinking of.¹²³

Additionally, the analysis unit should be the people who answer the phone when field companies or EMS units discover things they consider suspicious and need to ask questions. They should be looking at reports. A department needs somebody who is really looking at terrorism around the world to answer phones or correlate reports.¹²⁴

This unit needs to ask the tough questions of a department, are they prepared? The intelligence unit, possibly in conjunction with the area's police department and local Protective Security Advisor should make of a list of potential terrorist targets. Look at the top 50 potential targets; it is not an insurmountable number.¹²⁵ The unit looks at the current fire department response and asks if there were a terrorist attack on this target, how would the response need to change? Where would water be obtained? How would members and the public be protected? What if there were multiple attacks, how

¹²³ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹²⁴ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

¹²⁵ John McCreary, interview by author, field notes, Washington, D.C., November 25, 2008.

would resources be obtained? This is not new; fire departments have been doing target hazard planning for years, this unit does the same thing except though the lens of terrorism.

The analytic unit needs to look at a community through the eyes of a terrorist. Often, homeland security analysts look at vulnerabilities. Exploring vulnerabilities may not be the best way to discover potential targets for response planning. Just because a potential infrastructure target is vulnerable does not mean a terrorist is interested in it. "What do they like to attack? They go for sensational targets – headlines – not for fundamental and revolutionary change. If it is possible to see through terrorist eyes at what they would like to attack if they had their druthers, one would find it does not look like the list of vulnerable targets that law abiding analysts identify."¹²⁶ Therefore, another way to look at potential targets is through the use of attractors. "Because that is the only relevant starting point. What do they (the terrorists) see as viable, an attractive target? So, we developed . . . a set of attractors."¹²⁷ "We used 36 of the most sensational attacks in the world to come up with this alternative" to critical infrastructure vulnerabilities.¹²⁸ The attractors this research found were the following.

- Visibility – sensational press
- Essentiality – lack of workarounds
- Occupied -- lots of people
- Accessibility – easy to get to
- Inter related – Multiple effects and big bang for the buck
- Symbolism – psychological impact¹²⁹

This list assists in looking at targeting from the eyes of an adversary; fire department analysts need to do the same thing.

¹²⁶ John McCreary, e-mail message to author, November 23, 2008.

¹²⁷ John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

¹²⁸ Ibid.

¹²⁹ John McCreary, "The Critical Infrastructure Warning Project," Booz Allen Hamilton, 2003.

In summary, analysis is performed by a small group of dedicated and mentally flexible individuals, three to four at most.¹³⁰ “You ‘right size’ it (the analytical unit) by asking the question how do I make certain that everything I receive . . . is seen by a small enough group that they can collate it.” Bigger is not better. It is better to have two people who know all the facts than ten people who each know one fact. In any event, this unit should have a steady supply of information coming in, and analyze it to see how or if it applies to the local community. These units should look at attacks around the world for lessons that can be used by the local fire department. They should look at potential targets in the community and plan a fire department’s response; they should be available to answer questions from field units and make contacts with other agencies in the area that are involved with homeland security. Analysis should support preparedness and pre-planning in a department.¹³¹ Ultimately, by their research and planning, they protect life and property in their local community.

E. DISSEMINATION

1. Information Transfer

The method of dissemination is the one place in the intelligence cycle for a fire department’s intelligence shop not to be imaginative. Almost all of those interviewed recommended that an intelligence office act through existing processes. This is especially true as an intelligence office comes on line; later the office may tweak the system, but it is initially easier to go through existing communication pathways. Mark Johnson stated, “So I would try to do it through the existing (communications processes), you don’t want to necessarily set up a brand new information sharing process. That may or may not be advisable depending on the situation but in general, most organizations, mature

¹³⁰ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

¹³¹ “Fire Department Intelligence Officer,” *FDSOA Safety-Gram* 15 (February 2007): 1.

organizations . . . already have their set way of doing things and trying to change it is sometimes not pretty.”¹³² In other words, do not make waves where waves are not necessary. Use the communication pathways that already exist.

A fire department intelligence unit needs to be discreet. Not all information should be sent to all members of the department. The intelligence unit will need to decide what intelligence is useful for the higher echelons of the department and what should go to the field companies. Intelligence that affects situational awareness should be sent to all levels of the department. In the Ventura Police Department, “we leave it to that (TLO) sergeant to decide if they are going to put that out to the troops or do a training bulletin or do some kind of notice or something that uh he feels or she feels is would be valuable for the street officer and then do through briefings you know roll calls and things like that.”¹³³

George Friedman recommends that the intelligence unit have “a method for disseminating it (intelligence) not only to the fire department but to the police department as well so that they can be alerted.”¹³⁴ It is also important to pass the information along to other parts of the department other than the field units. For instance, fire inspectors should be included because they are in various premises and are potentially valuable sources of additional information, if they know what they are seeking. Another division of the department that should be included in the information flow is training. Correct and up to date information should appear in training scenarios and training bulletins. Though discreet, dissemination should be as wide ranging as is necessary for the intelligence unit to fulfill its duty to protect life and property.

¹³² Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

¹³³ Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

¹³⁴ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

2. Feedback

Along with the written materials, the intelligence unit is disseminating some type of feedback form that should be included. It does not matter if the dissemination is electronic or paper, the consumer should have a chance to give comments on the materials received. This is a form of quality control. Remember the whole point of this intelligence process is to support the consumer of the product. If there is no feedback process, an intelligence unit will never improve the products it is putting out. "For each article that we (the Open Source Center) put up on our website anyone reading that can respond and ask a question, make a statement, whatever and once they hit the send button it comes to our customer service team who are not the experts but they will immediately pass it off to the author or someone else who knows about the subject matter."¹³⁵ An intelligence unit should not be afraid to ask if their materials were useful or how they could be improved.

Moreover, the feedback process allows consumers of intelligence to ask questions on the materials presented. One of the purposes of an intelligence unit is to educate the department they serve. Any request for additional information on the materials disseminated should be welcomed and be given a rapid response. If an intelligence unit does not have the information at hand, so inform the consumer right away. Then try to find the information requested. Being responsive earns a lot of good will for the intelligence unit.

Part of the feedback process is also to ask the department's senior managers and its firefighters what they feel they need to know. What information, what intelligence in their mind is lacking? Leave a space on the feedback form asking what the consumer would want to know about or feel is lacking in their understanding of terrorism. Bear in mind, the intelligence cycle is a cycle; the process is iterative. The issues department personnel want or need

¹³⁵ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

to know about are really nothing other than new requirements. Requirements are, of course, the first step of the intelligence cycle. These new requirements cause a new cycle of collection and the process continues.

IV. RECOMMENDATIONS

A. TRAINING

Every person interviewed stressed the need for firefighters in the intelligence unit to be properly trained. The interviewees may not have all agreed on how best to train a firefighter; however, training was stressed as one of the most important factors in the success of a fire department intelligence project. The methodologies ranged from mentoring to formal classroom training. Formal training can come from government or from academia, whereas mentors may be volunteers with an intelligence background coming out of the local community or a vendor hired for a limited period. Again, a department should not forget to see if they have personnel with a military intelligence background who might be willing to assist in the effort.

1. Formal Instruction

One good resource for training is the Open Source Center outside of Washington, D.C. Mark Johnson of the Open Source Center reported, "We offer training and we have a whole catalog of courses and perhaps a dozen of them are relevant to a person like at a fire department. We teach analytical, basic analytical methods and advanced analytical methods."¹³⁶ The courses themselves are free of charge. The local fire department pays associated travel costs.

Also at the federal level, the Department of Homeland Security's Office of Intelligence and Analysis offers training. The DHS "Intelligence Training Branch . . . has begun to develop homeland security-centric courses for our DHS intelligence personnel and our state, local and tribal partners at our own

¹³⁶ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

Homeland Security Intelligence Training Center in Ashburn, Va.”¹³⁷ The Basic Intelligence and Threat Analysis Course (BITAC) is a five-week course that awards a Homeland Security Intelligence Officer designation. Fire department personnel may take these courses at no cost and grant money may be provided to cover travel costs.

There may also be training available at a state or local level. For instance, the Department of Homeland Security offers courses in open source intelligence through the State and Fusion Center Program office.¹³⁸ These programs provide training in open source tradecraft. “We call it tradecraft, it's how to analyze, how to evaluate sources, it's basically teaching you common sense methods in understanding the information coming at you and separating the fluff from the real, (find) the good stuff and then taking all those bits of information, laying them out on the table and then writing, describing what it is you are reading there, what are you seeing there and are there any judgments to be gained from that, and . . . where to get information.”¹³⁹ Some states may have a Terrorist Liaison Officer program available. Pat Miller recommended that departments “train some firefighters as Terrorist Liaison Officers” as a good way to start an intelligence program.¹⁴⁰

In addition, there are university programs that train people in intelligence. Mark Johnson stated,

There are a number of universities and colleges that have established intelligence educational curriculum. One that stands out in my mind is Michigan State University, Dr. Dave Carter, he teaches constantly. He is constantly on the road at police departments nationwide teaching open source methods, intelligence methods. He wrote papers on intelligence . . . these

¹³⁷ Charles Allen, “The Department Develops its Own Professional Intelligence Workforce,” *Leadership Journal*, January 14, 2009. <http://www.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html> (accessed February 7, 2009).

¹³⁸ Mark Johnson, interview by author, field notes, Washington, D.C., November 4, 2008.

¹³⁹ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

¹⁴⁰ Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

sorts of topics. So (you have the) Open Source Center at the federal level and then you got a few colleges and universities, Michigan State, I think Penn State has some, New Mexico, I heard about an intelligence program up there.¹⁴¹

There are also formal on-line training programs available. Fred Burton pointed out that the Bush School at Texas A&M has an on-line Homeland Security Department.¹⁴² Henley-Putnam University is accredited and is highly recommended.

Henley-Putnam has got the best tactical training courses that I have ever seen in an online format. And the FBI (and), for example, all the agents assigned as ATF analysts, have recognized this program as (the) one. If (FBI agents) want to take the courses there online, the FBI will pay for it. And, I mean they have (relevant) courses, courses, you know, not like English 101 or Writing 101. They have . . . Surveillance Detection Training . . . Strategic Analysis, Tactical Analysis courses, How Do You Do a Threat Assessment. And so, they've got some very good courses that also come with very good instructors and very good training manuals that, you know, and books and so forth that you get to refer back to.¹⁴³

These types of programs are of great benefit in a busy world because fire department members can take courses in analysis in an on-line format.

2. Mentoring

Several of those interviewed recommended mentoring as the best way of training fire department members as analysts. The idea would be that fire personnel would become a good analyst by working directly with and learning from a good analysts. George Friedman suggested, "The best way to train these guys is to attach them to an analyst doing work and make them his assistant for three months. You know go get me coffee, go Xerox this, go check this fact out, go check that fact out. And then you see it's really a master craftsman working

¹⁴¹ Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

¹⁴² Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹⁴³ Ibid.

as apprentice. And in due course he becomes quite good.”¹⁴⁴ Some successful private intelligence agencies train their new analysts in this fashion; they believe mentoring is superior to formal training because their new analysts learn to avoid the restrictive hard and fast rules of the American intelligence community.¹⁴⁵

There are several ways a mentoring program could be initiated by a department. As was written earlier, a department may have internal resources such as former military intelligence veterans who might mentor personnel in a departmental intelligence unit. The first step, then, is to check within one’s own department. The next step is to check one’s community. Are there military facilities that might help put a department in touch with retired intelligence officers? Lastly, as mentioned previously, several intelligence associations have offered to set-up an intelligence mentor with a local fire department.

B. KEEPING IT REAL

Many of the interviewees stressed the need for a new analysis unit to “keep it real.” Though this was mentioned before, it is worth repeating, the intelligence produced by the new unit must be related to the operations of that department. It has to have clear value. If city or department administrators are to support this project, they must see real value. Real value comes from the analysis unit improving their department. If the intelligence produced is not actionable, the unit will lose support. “Write what the department needs. You might do great writing, but it’s not on a topic that anyone needs it is worthless.”¹⁴⁶ Similarly, John McCreary commented on the intelligence generated by a fire department intelligence unit, “There is real value to this if there is information that is relevant to your mission.”¹⁴⁷

¹⁴⁴ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

¹⁴⁵ Ibid.

¹⁴⁶ Ibid.

¹⁴⁷ John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

Look at areas in the department that have a potential to fail in the event of a terrorist attack, work at improving those areas. Do the homework. If it is not known, then admit as such. Do not make up answers. "Credibility is golden, if you don't know, say so. Try to find the answers."¹⁴⁸ Once an intelligence unit's credibility is gone, it is dead in the water. Chances are it will never get its credibility back.

If an intelligence unit does good analysis and writing, it will be noticed. "When your intelligence department writes something that probably would be unusual, but in many ways brilliant, the battalion chief when he reads that report . . . is going to say, 'Wow. I want more of that.' And word of mouth itself would grow that section (analysis unit)."¹⁴⁹ Keep the unit's research real, keep it relevant, and keep it credible. If a department is going to form an intelligence unit or even if it is only one intelligence officer, Fred Burton summarized the mandate of this initial phase of the project well, when he said, "You have a limited window to impress. Don't waste it."¹⁵⁰

¹⁴⁸ George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

¹⁴⁹ Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

¹⁵⁰ Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

A. PROPOSITIONAL MODEL

The research shows there are definitive relationships between the Aggregated Second Order Codes. First, the entire fire intelligence process must be surrounded with integrity and usefulness. These are the same values that govern the fire service on a day-to-day basis. These mandatory overarching values will keep the intelligence unit in operation and supported by their department. This second order code is called “Keeping it Real” and it encircles all others. Within that context, intelligence must be understood as a process and all the other aspects of the research are, therefore, contained within the second order code “Intelligence.” The process begins with “Requirements.” Someone or some committee must decide what a department needs to know. Some interviewees recommended against a formal requirement system and argued to allow the analysts themselves to decide what a department needs to know. However, some individual or group of individuals must make that determination and that is “Requirements.”

From the requirements, the intelligence unit begins to bring together the requisite information and intelligence; this second order code is called “Collection.” The collected materials then undergo “Analysis.” The analytical process is where an intelligence unit asks, among other questions, what does this fact or event mean to this particular fire department. How will it affect operations? Will it endanger citizens, firefighters, fellow first responders? The analytical product is then sent out to those who need the information it contains. This process comes under the second order code “Dissemination.” Part of the dissemination process is the allowance for feedback from the consumer. The questions contained in the feedback may lead to new requirements. “Training” improves the ability of the intelligence to recognize a department’s requirements. Additionally, good training improves collection and analysis by the intelligence unit.

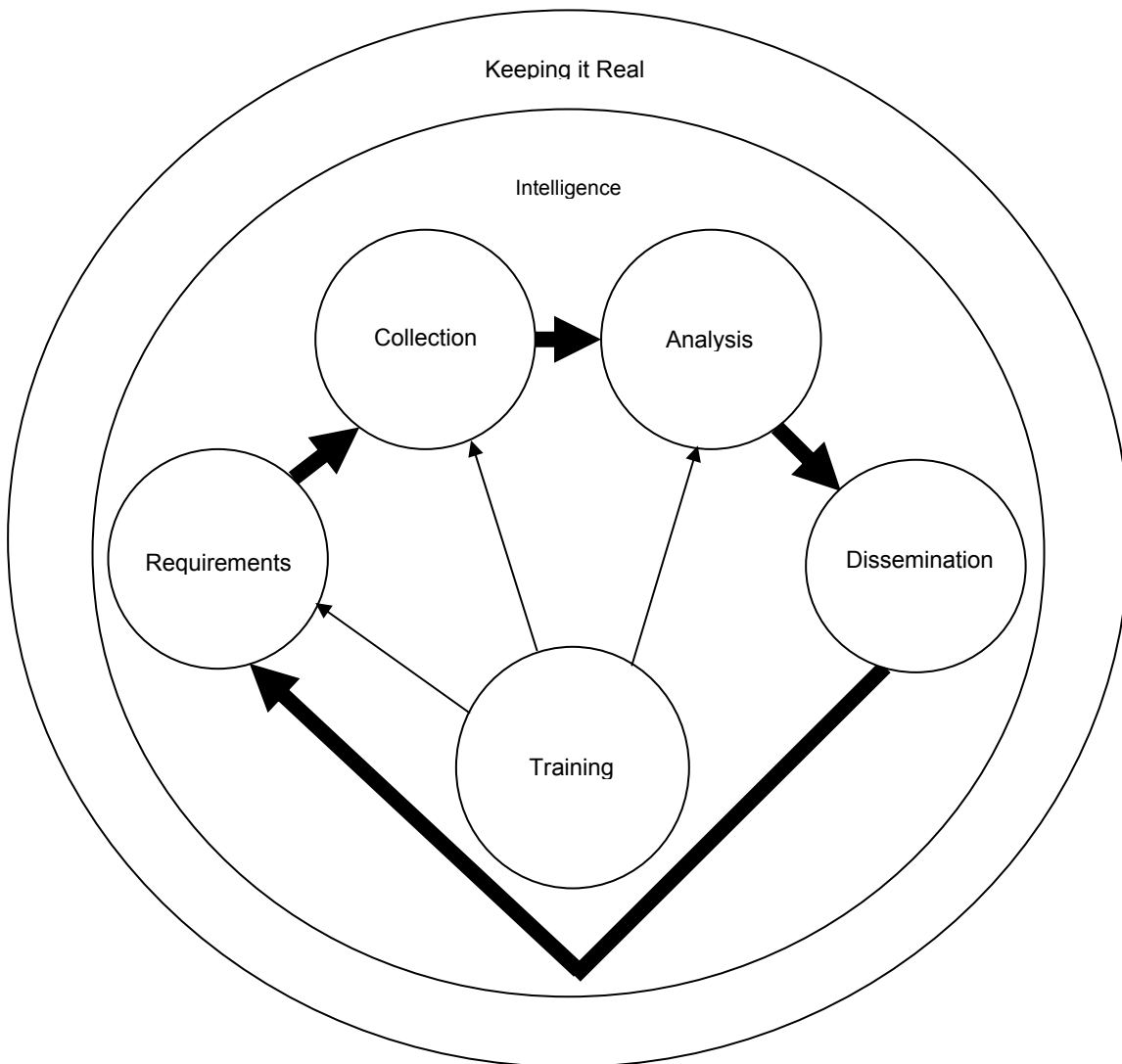


Figure 3. Propositional Model

B. INTELLIGENCE IN THE FIRE SERVICE

Those interviewed in this study clearly understood the need for fire departments to have their own intelligence officers or units. Everyone involved in this project was eager to help the fire service develop the skills and systems necessary to execute this vital work because they saw that need. No one, not the fusion center, not the local police, not federal agency can understand what a piece of intelligence means to a particular fire department with a particular set of procedures in a particular locale. Only the local firefighter has that wisdom. For

that reason, every fire department should have personnel trained in intelligence and informing their department on terrorism. This is not just the conclusion of this research. The Fire Department Safety Officers Association (FDSOA) also recommends that every department have an intelligence officer.¹⁵¹ Terrorism threatens both the lives of the citizens a department is sworn to protect and the firefighters themselves. Protecting life and property is the reason a fire department exists. An intelligence officer or unit helps a department fulfill that sworn duty.

¹⁵¹ "Fire Department Intelligence Officer," *FDSOA Safety-Gram* 15 (February 2007): 2.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Allen, Charles. "The Department Develops its Own Professional Intelligence Workforce." *Leadership Journal*, January 14, 2009, <http://www.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html> (accessed February 7, 2009).
- Benavides, Ben. U.S. Army Intelligence Center. *Targeting Tomorrow's Terrorist Today (T⁴) through Open Source Intelligence (OSINT): Quick-Links Starter Handbook for the Open Source Analyst*. Fort Huachuca, January 2007.
- Blatus, Richard J. *Altering the Mission Statement: The Training of Firefighters as Intelligence Gatherers*. Master's Thesis, Naval Postgraduate School, 2008.
- Bush, George. *Executive Order 13356: Further Strengthening the Sharing of Terrorism Information to Protect America*. Washington, D.C., The White House, October 25, 2005. <http://www.whitehouse.gov/news/releases/2005/10/print/20051025-5.html> (accessed July 11, 2008).
- Calder, Rich and Murray Weiss. "Stash 'Bagged' at Market." *New York Post*, April 27, 2005.
- Cloud, Rosemary. *Future Role of Fire Service in Homeland Security*. Master's Thesis, Naval Postgraduate School, 2008.
- Corbin, Juliet and Anselm Strauss. *Basics of Qualitative Research*. 3rd ed. Sage Publications, Thousand Oaks, CA, 2008.
- Dabruzzi, Kyle and Daveed Gartenstein-Ross. "Firefighters' Developing Role in Counter Terrorism." *Policing Terrorism Report* 3 (July 2008).
- "Fire Department Intelligence Officer." *FDSOA Safety-Gram* 15 (February 2007): 1-4.
- Fire Department, City of New York (FDNY). *FDNY-DHS Intelligence Enterprise: Phase II Work Plan 01 April 2007 – 01 October 2007*. New York, March 2007.
- Fire Department, City of New York (FDNY). *Terrorism and Disaster Preparedness Strategy*. New York, 2007.
- Fire Service Intelligence Enterprise. *Progress Report 1*. December 28, 2007.

- Heuer, Richards J. *Psychology of Intelligence Analysis*. Washington, D.C., Center for the Study of Intelligence, 1999.
- Jardines, Eliot A. Office of the Director of National Intelligence. *National Open Source Enterprise*. Washington, D.C., April 2006.
- Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 3rd ed. Washington, D.C.: CQ Press, 2006.
- North Atlantic Treaty Organization. *NATO Open Source Intelligence Reader*. February 2002.
- North Atlantic Treaty Organization. *NATO Open Source Intelligence Handbook*. November 2001.
- Rubin, Herbert J. and Irene, S. Rubin. *Qualitative Interviewing: The Art of Hearing Data*. 2nd ed., Sage Publications, Thousand Oaks, CA, 2005.
- Sims, Jennifer, and Burton Gerber, eds., *Transforming U.S. Intelligence*. Washington, D.C.: Georgetown University Press, 2005.
- Stalder, Felix, and Jesse Hirsh. "Open Source Intelligence." *First Monday*, 7, no. 6 (June 2002), http://www.noemalab.org/sections/ideas/ideas_articles/pdf/stadler_hirsh_opensource.pdf (accessed April 18, 2008).
- Steele, Robert David. *Open Source Intelligence: Executive Overview*. Global Intelligence Partnership Network, January 1, 2004. <http://www.oss.net/>, (accessed April 18, 2008).
- Thomas, Gail Fann. "Research Methods: Qualitative Data Analysis." https://www.chds.us/courses/file.php/279/lecture_transcript/6-res_methods_qual_datas_analysis_transcript.doc?forcedownload=1 (accessed January 22, 2009).
- U.S. Congress. House of Representatives. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security. *Using Open Source Information Effectively*. 109th Cong., 1st sess., June 21, 2005.
- U.S. Congress. Senate. Select Committee on Intelligence. *Intelligence Reform and Homeland Security Intelligence*. 110th Cong. 1st sess., 2007.
- U.S. Congressional Research Service. CRS Report for Congress. *Open Source Intelligence (OSINT): Issues for Congress*. Washington, D.C., updated January 28, 2008.

- U.S. Department of Justice. Bureau of Justice Assistance. *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, D.C., September 2005. <http://www.ncjrs.gov/pdffiles/bja/210681.pdf> (accessed July 7, 2008).
- U.S. Department of Justice. Bureau of Justice Assistance. *The National Criminal Intelligence Plan*. Washington, D.C., June 2005. http://www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf (accessed July 10, 2008).
- U.S. Department of Homeland Security. Lessons Learned Information Sharing. *LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process*. December 2005.
- U.S. Department of Homeland Security. Office of Intelligence and Analysis. *Open Source for Fusion Center Practitioners*. n.d.
- U.S. Department of the Army. *Open Source Intelligence FMI 2-22.9*. Washington, D.C., December 5, 2006.
- Weeks, Douglas M. *Strategic Changes for the Fire Service in the Post-9/11 Era*. Master's Thesis, Naval Postgraduate School, 2007.
- Werner, Charles. "Progress Report: Information, Intelligence for the Fire Service." *Firehouse* 29 (December 2004): 40-42.
- Wilson, Michael R. "Intelligence Units Reduce Arson." *Fire Chief* 32 (August 1988): 46-49.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Chief of Department Salvatore Cassano
Fire Department, City of New York
Brooklyn, New York
4. Assistant Chief Joseph Pfeifer
Fire Department, City of New York
Brooklyn, New York